NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

U.S. NATIONAL CYBERSTRATEGY AND CRITICAL INFRASTRUCTURE: THE PROTECTION MANDATE AND ITS EXECUTION

by

Scott T. Roper

September 2013

Thesis Advisor: Dorothy E. Denning
Co-Advisor: Edward L. Fisher

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE U.S. NATIONAL CYBERSTRATEGY AND CRITICAL INFRASTRUCTURE: THE PROTECTION MANDATE AND ITS EXECUTION		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Scott T. Roper			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The U.S has experienced numerous strategy assessments, with respect to cybersecurity of the national critical infrastructure and key resources (CI/KR). This is primarily due to the recurring realization of, but failure to address, root issues creating a clear disparity between the strategic national requirements and DHS' execution of its mandate regarding the reactionary protection of CI/KR.

This thesis compiles: (1) the current and past literature involving the evolution of critical infrastructure protection, as it relates to cybersecurity; (2) how the current administration is addressing it; and (3) the various roles and authorities allocated to the various major executive agencies.

This thesis concludes by providing eight specific recommendations with respect to improving the cybersecurity of the national CI/KR.

14. SUBJECT TERMS strategy, cyber, cyber-attack, cyber policy, cyber era, USCYBERCOM, US-CERT, national cyber strategy, national infrastructure protection plan, NIPP, critical infrastructure, CI, key resources, KR, CIKR, CI/KR, critical infrastructure protection, CIP			**15. NUMBER OF PAGES** 161
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

U.S. NATIONAL CYBERSTRATEGY AND CRITICAL INFRASTRUCTURE: THE PROTECTION MANDATE AND ITS EXECUTION

Scott T. Roper
Lieutenant Commander, United States Navy
B.S., Excelsior College, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author: Scott T. Roper

Approved by: Dorothy E. Denning
Thesis Advisor

Edward L. Fisher
Co-Advisor

Cynthia E. Irvine
Chair, Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The U.S. has experienced numerous strategy assessments, with respect to cybersecurity of the national critical infrastructure and key resources (CI/KR). This is primarily due to the recurring realization of, but failure to address, root issues creating a clear disparity between the strategic national requirements and DHS' execution of its mandate regarding the reactionary protection of CI/KR.

This thesis compiles: (1) the current and past literature involving the evolution of critical infrastructure protection, as it relates to cybersecurity; (2) how the current administration is addressing it; and (3) the various roles and authorities allocated to the various major executive agencies.

This thesis concludes by providing eight specific recommendations with respect to improving the cybersecurity of the national CI/KR.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS:

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ARPANET	Advanced Research Projects Agency Network
C2	Command and Control
CAS	Comprehensive Assessment System
CCIPS	Computer Crime and Intellectual Property Section
CI	Critical Infrastructure
CICG	Critical Infrastructure Coordination Group
CI/KR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CJCS	Chairman of the Joint Chiefs of Staff
CNA	Computer Network Attack
CNCI	Comprehensive National Cybersecurity Initiative
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNSS	Committee on National Security Systems
COP	Common Operational Picture
CS&C	Office of Cybersecurity and Communications
DCEO	Defensive Cyber Effects Operations
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DNI	Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
E^3A	EINSTIEN 3 Accelerated
EO	Executive Order
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency

FISA	Foreign Intelligence Surveillance Act
FRP	Federal Response Plan
GAO	Government Accountability Office
GIG	Global Information Grid
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
IA	Information Assurance
IC	Intelligence Community
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDC	Information Dominance Corps
IDS	Intrusion Detection System
IIMG	Interagency Incident Management Group
INS	Incidents of National Significance
IPS	Intrusion Protection System
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Providers
JP	Joint Publication
KR	Key Resources
NCCIC	National Cybersecurity and Communications Integration Center
NCCT	National Coordinating Center for Telecommunications
NCPS	National Cybersecurity and Protection System
NDCM	Non-Intrusive Defense Countermeasures
NDRF	National Disaster Recovery Framework
NIAC	National Infrastructure Assurance Council
NIAP	National Infrastructure Assurance Plan
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology

NORTHCOM	U.S. Northern Command
NPPD	National Protection and Programs Directorate
NRF	National Response Framework
NRP	National Response Plan
NSA	National Security Agency
NSCS	National Security Cyber Specialist
NSD	National Security Directive
NSDD	National Security Decision Directive
NSPD	National Security Presidential Directive
OCEO	Offensive Cyber Effects Operations
OMB	Office of Management and Budget
OUSD-P	Office of the Under Secretary of Defense - Policy
PCC	Policy Coordinating Committee
PCCIP	President's Commission on Critical Infrastructure Protection
PCIPB	President's Critical Infrastructure Protection Board
POTUS	President of the United States
PDD	Presidential Decision Directive
PPD	Presidential Policy Directive
RSF	Recovery Support Function
S&T	Office of the Science and Technology Directorate
SAP	Special Access Programs
SCADA	Supervisory Control and Data Acquisition
SECDEF	Secretary of Defense
SIEM	Security Information and Event Management
SIGINT	Signals Intelligence
SNRA	Strategic National Risk Assessment
SSA	Sector-Specific Agency
THIRA	Threat and Hazard Identification and Risk Assessment

UCP	Unified Command Plan
U.S.C.	United States Code
USACE	U.S. Army Corps of Engineers
USCYBERCOM	U.S. Cyber Command
USNORTHCOM	U.S. Northern Command
USSTRATCOM	U.S. Strategic Command
US-CERT	United States Cyber Emergency Response Team
WoN	Whole-of-Nation

ACKNOWLEDGMENTS

Dedicated to a great man and father who challenged me intellectually and drove me to become the man I am—John “Jack” Fredrick Gerke (04 March 1928—10 August 2013). He is missed already.

This journey has been an unexpected challenge. Managing to be an active father while navigating the challenges and triumphs of a graduate program, and trying to maintain some impression of normalcy in my personal life seemed like an unattainable goal at times. Looking back now though, it is the contributions of my colleagues that created such an incredible and memorable experience. With that, I thank and acknowledge my classmates who joined me on this journey. This program united the most fascinating and wonderful cast of characters. I also want to thank the professors for guiding us through the rigorous curriculum and encouraging us to explore issues through various prisms. Specifically, I would also like to thank the following list of amazing people whose assistance, support, and contributions made this thesis a reality:

- Dorothy Denning, from the Naval Postgraduate School (NPS) for her quiet patience and confidence in my drive. Without her direct involvement, and deep insight in the field of cyber, this thesis would not have been possible.
- Edward Fisher, from the Naval Postgraduate School (NPS) for his guidance, support, trust, and encouragement in taking these ideas and concepts and turning them into a worthwhile opportunity.
- Last, but most importantly, to my loving and beautiful wife, Jannelli, for her encouragement, love, tolerance, and understanding during the late nights of studying, working through problems, revising this thesis, and balancing the coordination needed for: (1) Piano; (2) Soccer/Baseball; (3) Cubmaster Cub Scout Pack-135; (4) Hospitality Volunteer at church; and (5) being a husband, father, and son.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Sir Francis Bacon's most famous and oft quoted aphorism dates back to publication in a chapter called Of Heresies in his book *Meditationes Sacrae* (Sacred Meditations) published 1597. While not the first to realize this universal truth, he nonetheless is attributed with encapsulating the crux of social dominance with just these simple words which were added into his essay in parenthesis, almost as an afterthought —"… for knowledge itself is a power..." (Bacon, 1597, M5). Truncated by many through the ages and taken out of the religious context in which it had been written, this phrase has popularly come to be known simply as: *knowledge is power*. Few historic examples can compare to the lengths by which this phrase has been demonstrated than that observed through the manipulation of code, via the supervisory control and data acquisition (SCADA) targeting computer worm coined STUXNET in June 2010. Although essentially degrading the nuclear enrichment program of a nation-state, more importantly this event solidified the reality that the cyber domain is operational and can have very real effects on the physical world, while retaining a measure of anonymity and without necessarily placing military combat units on foreign soil. This physically destructive demonstration, once made globally known by Iran, encapsulated and epitomized the fears of many self-aware nation-states around the globe as they internalized the security vulnerabilities inherent in an interconnected and globally driven economy. These fears and concerns are not exclusively an external problem; the United States (U.S.) has been aware of this vulnerability and attempting to mitigate it for decades.

> Increasing computer interconnectivity, such as the growth of the Internet, has revolutionized the way our government, our nation, and much of the world communicate and conduct business. However, this widespread interconnectivity poses significant risks to the government's and the nation's computer systems, and to the critical infrastructures they support. These critical infrastructures include systems and assets—both physical and virtual—that are essential to the nation's security, economic prosperity, and public health, such as financial institutions, telecommunications networks, and energy production and transmission facilities. (GAO-11–865T, 2011, p. 1)

As early as July 1995, a U.S. National Intelligence Estimate predicted future terrorist attacks against the U.S. and specified that the White House, the Capitol, symbols of capitalism (e.g., Wall Street), critical infrastructure (e.g., power grids, water distribution), areas where people congregate (e.g., sports arenas, malls), and civil aviation were generally considered suitable targets of vulnerability (National Commission on Terrorist Attacks, 2004, p. 341).

A. SCOPE OF WORK

> It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems. (Presidential Decision Directive 63, 1998, para. II)

This thesis is solely intended to document the ongoing U.S. national strategy evolution and implementation with respect to national protection of the cyber integrated critical infrastructure (CI) and key resources (KR). Specifically, this thesis focuses on reviewing and documenting the history, authorities and responsibilities aligned at the national level with regard to defense of the nation against a cyber-threat to national CI/KR.

While primarily focusing on Department of Homeland Security (DHS) and Department of Defense (DoD), it will also explore and identify additional agencies with active mandates or roles in cyber defense of the nation. When a holistic view has been established, and gaps have been identified, recommendations to bridge the gaps are made. This thesis concludes with a viable, although not necessarily palatable, recommendation for restructuring authorities and responsibilities in order to best mitigate attacks from antagonists utilizing a cyber-strategy and identifying the organization or agency best suited to be the federal lead in protecting cyber systems integrated with CI.

B. PROBLEM STATEMENT

"The capability to do harm—particularly through information networks—is real; it is growing at an alarming rate; and we have little defense against it" (Critical

Foundations, 1997, p. i). The above quote was taken from the a letter written to the U.S. President by Robert T. Marsh, Chairman of the President's Commission on Critical Infrastructure Protection, when he presented the Commission's findings in 1997. Frustratingly, few can effectively argue that we, as a nation, have adequately met that threat as it has grown exponentially. Both U.S. presidents since have struggled with the same issue and directed a review, received a report of findings, and issued strategic guidance in the form of national policy.

> Defense Secretary Panetta stated that 'foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country. We know of specific instances where intruders have successfully gained access to these control systems. We also know that they are seeking to create advanced tools to attack these systems and cause panic and destruction and even the loss of life. (Rogers, 2013)

In-line with current and future conflict, the National Military Strategy for Cyberspace Operations (2006) highlights the increasing complexity of the weapons and command and control which is forcing more reliance on operations in cyberspace. Domestically, information systems are increasingly used in the control and remote monitoring of critical infrastructure (CI), and as such present themselves as attractive asymmetric targets to adversaries. This is troublesome since irrespective of the period of battle or the designated leader, commanders of any size force entering conflict through the ages have always faced the same antagonists of war—space, force, and time. The dilemma in our newly emerging *cyber-era* is that the space dimension is too expansive to be clearly defined and thus neither a nation-state nor a singular organization is truly able to face/manage cyber threats as an independent entity.

C. PURPOSE OF STUDY

The global architecture of networks, along with the infinite number of system administrators, makes it impossible to isolate a threat within organizationally or territorially-defined jurisdictions. As such, this thesis will look at the initial and ongoing

domestic efforts to secure national critical infrastructure and key resources (CI/KR) with respect to cyberspace.

Possibly best captured early in the cyber revolution and codified in law, the Critical Infrastructures Protection Act of 2001 states that the official U.S. policy is that "… any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States" (42 U.S.C. 5195c, sect. c(1)).

This study is intended for the Office of the Under Secretary of Defense for Cyber Policy, the DHS, and the DoD U.S. Cyber Command to aid in properly assessing the necessity of the realignment of responsibilities between federal organizations, specifically between the DHS and the DoD in primary protection of national CI/KR. As such, this work is intended to contribute to the strategic level discussion of national cyber policy.

1. DoD Applicability

The DoD utilizes national cyber strategy, policy, and intent for fiscal planning, in order to properly align increasingly scarce allocated resources in the defense of the nation, in accordance with the National Military Strategy. Specifically, incorporation efforts by DoD aim to identify necessary structure and liaisons in order to reduce response times in crisis situations, ensure continuity of communication, and to increase efficiencies in support of national strategic objectives. Thus, by recommending a more stream-lined national response structure, with respect to threats emanating from or through the cyber domain, this study's recommendations, if implemented, may directly impact the DoD by shortening the national response time to cyber-related threats to CI/KR.

Explicitly, the DoD, via U.S. Northern Command (NORTHCOM), would benefit from a more efficient cyber situational awareness of CI/KR structure as it may reduce evaluation time required to provide an accurate assessment to the U.S. president. Presently, NORTHCOM is tasked via the Unified Command Plan with determining and

advising the U.S. president if the nation has met the necessary threshold to be considered under *attack*, and thus an indicator of potential conflict/war, domestically.

2. U.S. Navy Applicability

The U.S. Navy Information Dominance Corps (IDC) may directly benefit from this work, as the operational lead for evaluating and providing a professional judgment to the NORTHCOM Commander, with respect to whether the attack threshold(s) for the homeland has been exceeded, is currently a U.S. Navy IDC Flag Officer. Better situational awareness of the national cybersecurity environment and posture will better enable sound judgments and recommendations by decreasing uncertainty and therefore risk.

3. NPS Applicability

Though not all inclusive of all material available to date, this thesis compiles significant cyber-related documentation into a single source, within the chronological timeframes and national intent in which it should be considered. As such, this thesis can add to the focused national cyberstrategy and cyber policy discussions necessary in applicable degree programs at the Naval Postgraduate School (e.g., Cyber Systems and Operations).

D. LIMITATIONS

Significant impediments remain as obstacles in a candid discussion on the topic of cyber authorities and responsibilities. A few of the impediments are seen as restraints in this thesis. These are namely the unclassified discussion of cyber capabilities (as it relates across the full spectrum of cyber lines of operation), lack of a nationally accepted and implemented lexicon, and political restraints.

1. Capabilities

Due to the highly classified nature of the DoD cyber Special Access Programs (SAP), little in the way of capabilities will be delved into in an effort to keep the propensity of this thesis at the lowest level of classification possible. As such, it will be

grossly assumed that DoD, by the very nature of schools, billets, commands, and funding has the necessary means to employ and/or build the requisite capabilities needed for employing Offensive Cyber Effects Operations (OCEO) in the cyber domain.

2. Lexicon

To exacerbate the confusion, as of 2011 in the DoD alone, 16 Joint Publications (JP) discuss cyberspace-related topics and 8 mention cyberspace operations; complaints were that none contained a sufficient all-encompassing discussion of cyberspace operations (GAO Report 11–75, 2011). With the significant emphasis on cyber, DoD recognized the need to develop and update cyber-related joint doctrine and debated the merits of developing a single cyberspace operations joint doctrine publication in addition to updating all existing doctrine (GAO Report 11–75, 2011). As reinforcement, Mulligan and Schneider (2011) point out that without a widely accepted doctrine, evaluation of proposals for cybersecurity improvement is difficult, and debate about their implementation can be neither compelling nor conclusive. As a nascent overture, the initial lack of clarity regarding basic terminology was resolved internal to DoD with the revision of the JP 1–02 in May 2011, which officially defined cyberspace operations as "… the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace." More recently, in February 2013, the Chairman of the Joint Chiefs of Staff (CJCS) released the approved JP 3–12 publication which establishes the definitive cyber lexicon internal to DoD, as deconflicted with the Presidential Policy Directive 20 (PPD-20) which was released months earlier in November 2012 and introduced new terminology relating to the cyber domain (CJCS, 2013; POTUS, 2012).

U.S. Cyber Command actually went a step further by defining full-spectrum cyber operations as the employment of the full-range of cyberspace operations to support combatant command operational requirements and the defense of DoD information networks, to include Computer Network Defense (CND), Computer Network Attack (CNA), and Computer Network Exploitation (CNE) (GAO Brief 11–695R, 2011).

3. Political Solutions

Although many nation-states have developed and implemented alternate solutions for wrestling with the same issue of national cybersecurity, it is important to note the degree of control and public input in those decisions. As a single example, although seemingly brilliant in the design to maximize control and access to information from certain foreign sites for censorship purposes, the *Great Fire Wall* that is imposed in China is an untenable idea in the U.S. due to our inherent belief in individual freedoms and civil rights. Thus, it would be unwise to assume that the U.S. could unilaterally impose any strategy or doctrine to address any of the myriad of cyber challenges if it relied on similar civil-rights infringing properties, as the two political systems are so inherently different. With this acknowledgement, I limit the following work to the realm of reality that the U.S. solution must be viable within the current realm of the political system and therefore a self-imposed limitation, but one worth noting.

E. METHODOLOGY

The primary research method used to develop this thesis, providing the basis of knowledge and expertise, was a literary review.

I conducted a literature review of books, publications, U.S. and foreign law and policy, journals, Internet articles, and previous graduate and undergraduate research.

To determine the extent to which the U.S. government has issued updated and comprehensive guidance, I also reviewed national homeland defense and civil support doctrine, policy, and strategy and other relevant documentation, and met with officials from DoD and DHS to discuss the existing departmental guidance and to assist in identifying any potential gaps in the guidance that could exist.

Explicitly, I assessed national-level and DoD homeland defense and civil support guidance against emerging issues in discussions with DoD, combatant command, and military service officials including the dual-status commander construct and domestic cyber.

F. OUTLINE

This thesis is organized into the following chapters:

- Chapter I provides the introduction and overview of the thesis.
- Chapter II describes the significance of, and reviews, the historical context of the U.S. national strategy toward national protection and defense of critical infrastructure.
- Chapter III outlines the current implementation of national strategy in place to deal with threats to the national critical infrastructure—unity of effort.
- Chapter IV describes the legal authorities, roles and efforts of the federal agencies in the implementation of the current unity of effort strategy. There is also a discussion on the various strengths and weaknesses associated with each U.S. Code cited.
- Chapter V identifies the analysis of gaps in national documents, cyber authorities, and responsibilities and provides a conclusion.
- Chapter VI details specific recommendations and future research.

II. NATIONAL STRATEGY

> Perhaps the sentiments contained in the following pages, are not yet sufficiently fashionable to procure them general favor; a long habit of not thinking a thing wrong, gives it a superficial appearance of being right, and raises at first a formidable outcry in defence of custom. But the tumult soon subsides. Time makes more converts than reason. (Paine, 1776)

Commanders in any conflict, where an adversary operates, must manipulate the time controls over the decision making process to be successful in operations (Joint Publication 3–0, 2008). This theory is double-edged: 1) internalizing the goal of the seamless Command and Control (C2) process, friendly forces must reduce the uncertainty with which commanders must deal to expedite the decision of action; while 2) obfuscating the certainties and information needed by the opposing force to make accurate timely decisions (Coakley, 1991). Although the former is usually implemented through the use of *unity of command*, it is only a viable strategy when that command is empowered with the proper authorities to address the responsibilities it has been directed to execute. When that precondition is untenable or otherwise unavailable, the strategy of leveraging as many specialized and independent entities (with existing authorities) working toward a common stated goal may yield the same results. Therefore, it is important to note that absolutes should not exist in any direct application of theory since there are times where decentralization of authority can actually contribute to responsiveness by reducing the distance, whether in time and/or space, between decision makers and ongoing operations (Joint Publication 3–0, 2008). Deferring to this alternate strategy, and due to the sheer interconnectivity and specializations in each of the already legally established federal organizations, early in the cyber revolution the U.S. implemented a *unity of effort* strategy toward cybersecurity. The last three U.S. presidents have reaffirmed the decision to use a unity of effort approach which is demonstrated through the review of the federal documents in this chapter. Unity of effort is synonymous with a phrase commonly captured in Federal documents in the last ten years—whole of government approach. This strategy when implemented, regardless of

the actual term used, may be possibly sufficient in addressing nascent concerns of the fledgling interconnected autonomous systems.

A. SIGNIFICANCE

> The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems. … Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy. (Presidential Decision Directive 63, 1998, sect. I)

The above quote remains valid even 15 years later and represents an ill-addressed national priority, which could realistically be the U.S.' Achilles heel. Almost eleven years and three presidential administrations later, U.S. President Barrack H. Obama even highlighted, in a speech given May 29, 2009, that the "… cyber threat is one of the most serious economic and national security challenges we face as a nation" (Obama, 2009). The challenge obviously is one of leadership and reviewing or challenging the status quo. Therefore, the correct solution to defending our nation's critical infrastructure and key resources (CI/KR) from the cyber threat must begin with understanding what has been done to date by those entrusted to provide that protection and defense.

The U.S. Constitution empowers the Office of the U.S. president with authority and the responsibility to defend the nation. In that vein, due to the size and complexity of the task, the presidential responsibility has been delegated in many reformative documents as new and emerging threats are identified. The most recent of these threats is that of a cyber-attack affecting critical national infrastructure and key resources in an attempt to disrupt the American way of life.

1. Authority

In the propensity of the national security reformative documents released by the Executive Branch in the last 40 years, authority of the President in issuance is usually cited as being from the following key pieces of legislation:

(1) the U.S. Constitution;

(2) the Communications Act of 1934, as amended (47 U.S.C. 151);

(3) the National Security Act of 1947, as amended, the Defense Production Act of 1950, as amended (50 U.S.C. 2061);

(4) the Federal Civil Defense Act of 1950, as amended (50 U.S.C. 2251); and

(5) the Disaster Relief Act of 1974 (42 U.S.C. 5121 et seq.); Public Law No. 93–288, as updated by the Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988.

2. Reform

To date, much of the previous work on proactive national federal strategy to respond to *Incidents of National Significance* (INS) has been generated by the Executive Branch of the U.S. government in the form of various Executive Orders, National Security Decision Directives, Presidential Decision Directives, Homeland Security Presidential Directives, and Presidential Policy Directives. The key references later described in this chapter, spanning about 35 years, were created by multiple administrations with differing views and motivations, but naturally evolve from addressing general domestic invasion, to recovery from natural disasters, to man-made physical attacks, to now man-made cyber-attacks. Despite the shifting focus, what seems clear after reviewing the last 20 years' presidential directives and executive orders (EOs) is that all of the efforts seem circular in nature as each new presidential administration:

(1) identifies a critical vulnerability in the national defense of critical infrastructure;

(2) creates a committee of experts and insiders to research and evaluate issue; and

(3) then implements a personalized version of the unity of effort strategy.

The remainder of the chapter introduces key definitions, details the historic U.S. attempts to protect the national critical infrastructure and key resources, and finishes with a discussion of how the U.S. has performed successive strategy assessment cycles with respect to addressing cyber vulnerabilities.

B. COMMON TERMINOLOGY

As this thesis focuses on the federal strategy, policy and responsibilities surrounding the national protection of U.S. *critical infrastructure and key resources* (CI/KR) as it relates to a specific *incident of national significance* (INS) as identified by *national intelligence*, it follows that these terms should be defined to allow for contextual discussion.

1. Critical Infrastructure and Key Resources

Combined as a generic term, CI/KR essentially refers to assets crucial to national security, economic vitality, public health and safety. Multiple agencies have integrated the acronym into much of their literature. Although referring to the same sub-set of assets, the acronym is often seen both with and without the forward slash. Looking into it deeper, there seems to be no connotative difference, just agency or author preference. It is important to note that the two sub-terms embody different but not mutually exclusive sub-sets of national assets.

a. Definition

Although an evolving term in an equally evolving cyber-era, national *critical infrastructure* (CI) is formally reiterated/revalidated as of February 12, 2013 by the signature and release of Executive Order No. 13,636. The President of the United States (POTUS) defines critical infrastructure as "… systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Executive Order No. 13,636, 2013, p. 1). It is important to note that the CI definition presented in this EO is taken word for word from a document dated October 26, 2001—the Critical Infrastructures Protection Act of 2001 (42 U.S.C. §5195c, 2001, para. 1016(e)). This specific definition represents a significant deviation from more recent terminology/definition as it reverts to the previous definition and avoids specifically listing national critical infrastructure sectors, as nearly all subsequent definitions have attempted to include. In layman's terms, the acronym is generally indicative of national

power grids; water filtration plants and flow points; symbolic national monuments; critical government facilities; telecommunications and transportation systems; and chemical facilities.

For historical perspective and to highlight the struggle to correctly identify a definitive list, these earlier lists will be covered in the order by which the federal documents using them were released. Critical Infrastructure Protection (CIP) is one of the cornerstones of homeland security. Although Presidential Decision Directive 63 (1998) lists eight sectors, the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (2003) lists 11 sectors of CI, and the National Response Framework Critical Infrastructure and Key Resources Support Annex (2008) lists 17 sectors. Examples of sectors include but are in no way limited to: Water, Power & Energy, Information & Telecommunications, Chemical Industry, Transportation, Banking & Finance, Defense Industry, Postal & Shipping, Agriculture & Food, Public Health, and Emergency Services. The realization that, in a modern age, sectors previously under-integrated are now significantly important to the physical, financial, and health security of the nation simply highlights the transient nature of what can be deemed critical.

The term *key resources* (KR) remains more ambiguous and overshadowed by the fact that most critical infrastructure is better defined in documents previously released (e.g., National Infrastructure Protection Plan). As part of the Homeland Security Act of 2002 and reiterated in both the Homeland Security Presidential Directive 7 (2003) and National Infrastructure Protection Plan (2006), KR is described as "… publicly or privately controlled resources essential to the minimal operations of the economy and government" (6 U.S.C. §101, 2002, para. 9).

2. Incidents of National Significance

The Secretary of the Department of Homeland Security is the legal authority by which an INS is declared. This decision is made in coordination with other federal departments and agencies and is worked in conjunction with state, local, tribal, nongovernmental, and private-sector entity efforts. Formal INS designation allows for

unity of effort under DHS lead as they initiate actions to prevent, prepare for, respond to, and recover from such incident (National Response Plan, 2004). This term and authority of designation are not to be confused with the legal authority of the Commander U.S. Northern Command (NORTHCOM) to designate the homeland as being at war. Instead, it may be helpful in deconfliction of terms to understand that an INS would likely be the prelude to such a NORTHCOM designation.

a. Definition

The term INS seems to naturally follow as an evolution to the previous term in use by the federal government—*national security emergency*. Accordingly, the term national security emergency was originally introduced in Executive Order No. 12,656 on November 18, 1988 and was defined as "… any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States" (Executive Order No. 12,656, 1988, sect. 101(a)).

The term *incident of national significance* as first defined in the National Response Plan (2004), includes all presidentially-declared emergencies, major disasters, and catastrophes and directly references criteria provided in the Homeland Security Presidential Directive 5 (para. 4). Therein, INS is formally defined as, "… an actual or potential high-impact event that requires a coordinated and effective response by and appropriate combination of Federal, State, local, tribal, nongovernmental, and/or private-sector entities in order to save lives and minimize damage, and provide the basis for long-term community recovery and mitigation activities" (National Response Plan, 2004, p. 67). As the principal federal official for domestic incident management, the Secretary of Homeland Security declares Incidents of National Significance (in consultation with other departments and agencies as appropriate), which primarily include credible threats or acts of terrorism, major disasters, and emergencies (National Response Plan, 2004).

3. National Intelligence

National Intelligence initially is a difficult term to define in that it incorporates a word which has caused serious discussion and yet remains aloof in widespread lexicon acceptance—intelligence.

In the *Studies in Intelligence* journal, compiled and published by the Central Intelligence Agency (CIA), Dr. Michael Warner highlighted the disparity when he wrote, "In a business as old as recorded history, one would expect to find a sophisticated understanding of just what that business is, what it does, and how it works. If the business is 'intelligence,' however, we search in vain. As historian Walter Laqueur warned us, so far no one has succeeded in crafting a theory of intelligence" (Warner, 2007, p. 1). Although many have attempted it, and done so in the terms most desirable for their specific organization, few have succeeded in doing it in such terms as it remains viable across various organizations and agencies with different mandates and missions.

The DoD definitions often reference intelligence in terms of information of value as it pertains to enemy [*non-U.S.*] forces. So, although useful for combatting efforts of external antagonists, it negates a use internal to the U.S., when dealing with threats also generated internally. The CIA has a much broader purview and thus it may be that in 1999 they internalized the realization of domestically induced information may be the key to operationalizing information through the reduction of uncertainty. Thus in their definition, intelligence "… reduced to its simplest terms … is knowledge and foreknowledge of the world around us—the prelude to decision and action" (Central Intelligence Agency, 1999, p. vii).

a. Definition

In reference to Title 50 of U.S. Code (U.S.C.), as updated by the Intelligence Reform and Terrorism Prevention Act of 2004, the terms *national intelligence* and *intelligence related to national security* refer to all intelligence, regardless of the source from which derived. This designation expressly includes information, consistent with any guidance issued by the President, gathered within or outside the United States pertaining to multiple U.S. government agencies when the

stated information "… involves—(i) threats to the U.S., its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security" (50 U.S.C. §401a, 2004, sect. 5). As a result then, any threat to national CI/KR should be perceived by the executive agencies and shared as national intelligence.

C. THE ROAD TO ADDRESSING U.S. NATIONAL CRITICAL INFRASTRUCTURE CYBER VULNERABILITIES

Although the road to addressing U.S. critical infrastructure is a long one, chronologically listed below, and broken out under various U.S. presidential administrations, are simply a few of the more notable references which must be considered in order to understand and/or propose a solution to the issue of properly implementing a cybersecurity strategy at the national level.

1. President James "Jimmy" Carter's Administration

During President James "Jimmy" Carter's administration, prompted not by analysis but rather by the partial nuclear meltdown of one of the Three Mile Island nuclear reactors in Pennsylvania on March 28, 1979, he created, and then consolidated all presidentially vested powers for civil disaster response into a single agency for federal response to disasters—the Federal Emergency Management Agency (FEMA) (Executive Order No. 12,148, 1979, sect. 1).

a. Executive Order No. 12,127–Federal Emergency Management Agency (1979)

Days after the Three Mile Island accident, on March 31, 1979, Executive Order No. 12,127 was released marking a significant implementation of a previously approved plan. Reorganization Plan No. 3 of 1978 (43 FR 41943) established the Federal Emergency Management Agency, but it was Executive Order No. 12,127 which activated the plan and therefore set the date of FEMA activation as of April 01, 1979 (Executive Order No. 12,127, 1978, sect. 1–106).

b. Executive Order No. 12,148–Federal Emergency Management (1979)

Within four months of the Three Mile Island nuclear accident, on July 15, 1979, with continued significant concern over the lack of a viable national response to *civil emergencies* (a term preceding INS), Executive Order No, 12,148 was signed by President Carter. This EO significantly recalled and consolidated additional emergency management powers that were originally vested in the presidential authority but since delegated to organizations and agencies (e.g., Defense Civil Preparedness Agency, DoD, Federal Disaster Assistance Administration, Department of Housing and Urban Development, Department of Commerce, Federal Preparedness Agency, General Services Administration, Office of Science and Technology Policy) (Executive Order No. 12,148, 1979, sect. 1). This document is vital for two reasons: (1) it sets the precedence of significant authority consolidation, due to the concern generated over a single type of INS—nuclear and (2) it greatly empowered the primary federal agency still in place today responsible for coordinating a federal response to events which overwhelm state, tribal and/or local resources—FEMA.

2. President Ronald W. Reagan's Administrations

As it was at the fore-front of the political agenda, following the Three Mile Island accident in 1979, the threat of nuclear weapons use/attack domestically remained high on the national agenda as the arms race between the U.S. and Union of Soviet Socialist Republics (U.S.S.R.) ran its course. Central to that agenda was the survivability of national command and control through a national protection of the telecommunication systems. This concern was unambiguously addressed in a key document released during the first term of President Ronald Reagan, but was not the only significant document to emerge during his administrations.

Of historic note, it was also in 1983, during President Reagan's first administration, that the transition of the Advanced Research Projects Agency Network's (ARPANET's) Network Control Program protocol to that of the TCP/IP protocol

occurred, which is recognized by many scholars as the actual birth of the Internet as we know it today. The use of the interconnected computers greatly enhanced command and control and it is clear that it is in this context that his first administration sought to maximize its use during and after crisis situations.

President Reagan's second term in office is significant in that it produced an EO and key legislation both refining and clarifying the duties of the federal government in response to crises that exceed the capabilities of local, state and tribal resources.

a. Executive Order No. 12,381–Delegation of Emergency Management Functions (1982)

Released September 8, 1982, Executive Order No. 12,381 briefly clarifies and amends EO 12,148 as to authorities delegated to the FEMA. Specifically, this EO recalls previously delegated presidential authorities which were originally granted via the Disaster Relief Act of 1974 and clearly assigns them to FEMA. The first such recalled authority related to the declaration of emergencies and major disasters (Executive Order No. 12,381, 1982, sect. 1).

b. National Security Decision Directive No. 97–National Security Telecommunications Policy (1983)

Released June 13, 1983 as a classified document, the National Security Decision Directive No. 97 (NSDD-97) made specific allowance for both "… assured connectivity between the National Command Authority and military forces" and "… recovery of critical national functions following crisis situations" (National Security Decision Directive No. 97, 1983, p. 2). This document also created a steering group to oversee implementation of stated objectives and to liaise with the Federal Communications Commission, FEMA, and National Security Telecommunications Advisory Committee (National Security Decision Directive No. 97, 1983, p. 3).

c. Executive Order No. 12,656–Assignment of Emergency Preparedness Responsibilities (1988)

Signed on November 18, 1988, Executive Order No. 12,656 does exactly what its title suggests—assigns national security emergency preparedness responsibilities

to federal departments and agencies based primarily on "… extensions of the regular missions of the departments and agencies" (Executive Order No. 12,656, 1988, sect. 102(a)). The EO, in section 102(b), explicitly points out that it "… does not constitute authority to implement the plans prepared pursuant to this EO, but rather they could be acted on only in the event that authority for such execution is authorized separately by law." This EO updated and superseded two previous EOs which addressed national emergency responsibilities—Executive Order No. 10,421 (December 31, 1952) and Executive Order No. 11,490 (October 28, 1969). Additionally, this EO was released in conjunction with the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law No. 93–88, as amended by Public Law No. 100–707) and directs that each federal agency lead appoint a senior policy official to develop and maintain a "… multi-year, national security emergency preparedness plan for the department or agency to include objectives, programs, and budgetary requirements" (Executive Order No. 12,656, 1988, sect. 201(3)).

Together, the Stafford Act and Executive Order No. 12,656 lay the ground work for the development of the Federal Response Plan (FRP) to incidents of national significance. The primary difference between the verbiage of these documents and future documents lay in the supporting versus supported roles. In section 1702(1) of Executive Order No. 12,656 (1988), the Director of FEMA is directed to support other federal agencies in their preparation of national security emergency preparedness plans, whereas future documents shift the supported role to FEMA.

d. Robert T. Stafford Disaster Relief and Emergency Assistance Act (1988)

Still in force today, the Stafford Act, as it is commonly referred to, amended the Disaster Relief Act of 1974 (Public Law No. 93–288) as it related to federal government support of local, state and tribal efforts to recover from emergencies and disasters. Released November 23, 1988, the Stafford Act has received numerous revisions over the years since but still constitutes the statutory authority for most federal disaster response activities under FEMA.

3. President George H. W. Bush's Administration

Acknowledging that the presidential responsibilities were too vast to properly address as a lone individual using the current advisory councils, President George H.W. Bush (within days of inauguration) revitalized a standing advisory body of trusted advisors to aid him in the formation and reformation of national security. Despite this, catastrophic natural disasters in the late '80s and early '90s (e.g., the Loma Prieta earthquake, Hurricane Hugo, Hurricane Andrew and Hurricane Iniki) generated intense criticism of the U.S. federal response mechanism and prompted an investigation into the U.S. plans and efforts surrounding disaster response, as authorized via the Stafford Act of 1988 (U.S. Government Accountability Office Report No. GOA/RCED-93–186, 1993, p. 1). This criticism sparked national attention on the reformation of the U.S. national strategy to the protection of CI/KR.

a. National Security Directive No. 1–Organization of the National Security Council System (1989)

Released on January 30, 1989, National Security Directive No. 1 (NSD-1) refocused the advisory council still in use today by the President to aid in decision making and enforcement of standing national policy—National Security Council (NSC) (National Security Directive No. 1, 1989, p. 1). Refocused is the operative word, as the NSC was actually created during President Harry S. Truman's administration in 1947, but was viewed as an "… unwanted bureaucracy imposed upon the President by Congress" (Whittaker, 2011, p. 6).

NSD-1, in the NSC revitalization, dissolved and replaced the: National Security Planning Group; Senior Review Group; Policy Review Group; and Planning and Coordination Group (National Security Directive No. 1, 1989, p. 4). It was the intention that the NSC committees (i.e., Principles Committee, Deputy Committee, Policy Coordinating Committees) be the sole vessels to address crisis management vice "… a separate interagency structure" (National Security Directive No. 1, 1989, p. 5).

b. Executive Order No. 12,673–Delegation of Disaster Relief and Emergency Assistance Functions (1989)

Released March 23, 1989, Executive Order No. 12,673 delegated specific presidential functions to the Director of FEMA. This EO may look familiar as it is simply a near imitation of Executive Order No. 12,381, released seven years earlier and, like that EO, provided amendments to Executive Order No. 12,184 which empowered the Director of FEMA with functions previously granted to the President. The primary difference between the two EOs resides in the fact that Executive Order No. 12,381 delegated functions vested in the President by the Disaster Relief Act of 1974, and EO 12,673 delegated functions vested in the President by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) of 1988. It is important to note that both documents explicitly retain the presidential authorities to declare emergencies and natural disasters.

c. National Security Directive No. 10–Organization of the National Security Council System (1989)

Released on May 7, 1989, National Security Directive No. 10 (NSD-10) specifically created nine Policy Coordinating Committees (PCC) authorized via NSD-1 (National Security Directive No. 10, 1989, p. 1). This is significant as two of the nine PCCs directly relate to functions necessary post-cyber-attack on CI/KR and are still in use today. More specifically, the National Security Telecommunications PCC explicitly assumes the functions previously assigned via NSDD-97 to the National Security Telecommunications Policy Steering Group and is therefore responsible for continuity of communications between the military and the administration's National Command Authority (National Security Directive No. 10, 1989, p. 3). Additionally, the Emergency Preparedness/Mobilization Planning PCC (chaired by the Director of FEMA) focuses on domestic administration policy with respect to national security (National Security Directive No. 10, 1989, p. 2).

d. Executive Order No. 12,803–Infrastructure Privatization (1992)

Released April 30, 2009, Executive Order No. 12,803 remains one of the most controversial EOs signed. Under this EO, federally funded infrastructure assets owned by state and local governments are encouraged to be sold (aka: privatized) in order to "… ensure that the United States achieves the most beneficial economic use of its resources" (Executive Order No. 12,803, 1992). Examples of the infrastructure authorized for sale by states under Executive Order No. 12,803 include: roads, tunnels, bridges, electricity supply facilities, mass transit, rail transportation, airports, ports, waterways, water supply facilities, housing, schools, prisons, and hospitals (Executive Order No. 12,803, 1992, sect. 1(b)). This is significant as it further blurs the responsibility of the federal and state government to protect and/or defend critical infrastructure no longer owned by federal, state, or local governments.

4. President William J. Clinton's Administrations

The commercialization of the Internet in the mid-1990s, combined with a domestic terror act, provided the impetus for the U.S. government to refocus on the protection of CI/KR because of emerging cyber threats. Succinctly stated, "… because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy" (Presidential Decision Directive 63, 1998, p. 2).

a. Presidential Decision Directive 39–U.S. Policy on Counterterrorism (1995)

Following the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995, President William J. Clinton released Presidential Decision Directive 39 (PDD-39) on June 21, 1995. As such, PDD-39 directed the U.S. Attorney General to "… chair a Cabinet Committee to review the vulnerability to terrorism of government facilities in the United States and critical national infrastructure and make recommendations" back to the President (Presidential Decision Directive 39,

1995, p. 2). This event drove one of the first whole of government reviews of domestic vulnerabilities of the National Information Infrastructure (NII)—a term coined by the Information Infrastructure Task Force formed by Vice President Albert Gore (Security In Cyberspace, 1996, para. I(A)). The findings of the task force were later made public in a hearing by the U.S. Senate Permanent Subcommittee on Investigations, titled Security in Cyberspace (June 5, 1996). This is the document which began the shift away from a holistic focus on national CIP and eventually aided in breaking out very specific threats, such as cyber.

b. Executive Order No. 13,010–Critical Infrastructure Protection (1996)

As seen in the direct quote below from Executive Order No. 13, 010, released five weeks after the Congressional Hearing on Security in Cyberspace, the U.S. government was cognizant of and specifically concerned with the governance of the fledgling interconnected autonomous systems—i.e., the Internet.

> Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation. (Executive Order No. 13,010, 1996, p. 1)

This document is the first noted attempt to account for the vulnerability posed by the remote access to, and/or disruption of, critical infrastructure via cyber means and is clearly the start of the nation's struggle to implement an effective and palatable cybersecurity strategy to protect the nation's CI/KR. The use of the term *cyber threat* indicates a venue of attack to CI/KR and was not yet clearly included as part of CI,

as cyber networks are today. Regardless, due to these threats, President Clinton (through Executive Order No. 13,010) created the: 1) President's Commission on Critical Infrastructure Protection (PCCIP); 2) Principles Committee; 3) Steering Committee of the PCCIP; and 4) Advisory Committee to the PCCIP (Executive Order No. 13,010, 1996, p. 1–2). It is important to note that this was the first cited attempt to identify and state the national importance of CIP in light of the then coined phase—*Information Age*. The most critical observation to make though is the presidential identification and distinction of physical and cyber threats.

Under this Executive Order, President Clinton mandated the formation of the PCCIP and subsequent analysis of critical infrastructure in order to "… develop a strategy for protecting them and assuring their continued operation" (Executive Order No. 13,010, 1996, p. 1).

c. Critical Foundations: Protecting America's Infrastructure (1997)

Released in October 1997, the PCCIP's findings are titled *Critical Foundations: Protecting America's Infrastructure*. Primarily resultant to the majority of the infrastructure being privately owned and operated, the PCCIP concluded that CI protection is a shared national responsibility belonging to both the public and private sectors. Through this declaration, the PCCIP placed the protection of the nation's CI at the whim of disparate private sector companies whose nationalistic allegiances are not necessarily higher in priority than their drive for profit generation.

d. Presidential Decision Directive 63 (1998)

In response to the report from his Commission on Critical Infrastructure Protection, on May 22, 1998, President Clinton signed and released Presidential Decision Directive 63 (PDD-63). The directive, titled *Critical Infrastructure Protection*, was designed to defend the nation's critical infrastructure from physical and cyber-attack as identified in his previously released Executive Order 13,010 (1996). PDD-63 calls for a national effort to assure the security of the vulnerable and interconnected infrastructure of the United States (U.S.), most notably telecommunications. It went so far as to say, "…

the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber-attacks on our critical infrastructures, including especially our cyber systems" (Presidential Decision Directive 63, 1998, sect. II). This quote is significant as it shows a shift in thinking; PDD-63 explicitly includes cyber systems in CI, whereas just two years prior in, Executive Order No. 13, 010 (1996), it was only a threat vector to CI.

Additionally, PDD-63 is a significant milestone document as it is the first to identify, and assign Federal agency leads to, 15 critical infrastructure sectors (Presidential Decision Directive 63, 1998, sect. VI(1)). The CI/KR sectors, mainly still in use today, are listed in PDD-63 Appendix A (1998) as:

- Information and Communications,
- Banking and Finance,
- Water Supply,
- Aviation,
- Highways,
- Mass Transit,
- Pipelines,
- Rail,
- Waterborne Commerce,
- Emergency Law Enforcement Services,
- Emergency Fire Service,
- Continuity of Government Services,
- Public Health Services,
- Electric Power, and
- Oil and Gas (production and storage).

The foundation of PDD-63 stresses the critical importance of cooperation between the government and the private sector because the critical infrastructure of the U.S. is primarily owned and operated by the private sector (National Commission on Terrorist Attacks Upon the United States, 2004, p. 428). Note that this document also laid out a very specific goal of hardening our national critical infrastructure against intentional

attacks by the year 2003, via the creation of the Critical Infrastructure Coordination Group (CICG) (Presidential Decision Directive 63, 1998, sect. 2). This goal arguably has still not been met even 10 years after missing the deadline, but was very specific in the implementation guidance.

This document further advocates a unity of effort strategy, as the created National Coordinator position was expressly created to "… not direct Departments and Agencies," but rather simply to ensure interagency coordination for policy development and implementation. In essence, the National Coordinator was directed to implement and maintain a National Infrastructure Assurance Plan (NIAP), with no means of compliance incentivization. Additionally, to further the NIAP through unity of effort, the President directed the formation of the National Infrastructure Assurance Council (NIAC), which was later explicitly created under Executive Order No. 13,130, dated July 14, 1999, for the duration of two years.

5. President George W. Bush's Administrations

As should be expected, the terror attacks perpetrated against the U.S. mainland on September 11, 2001 (colloquially referenced as *9/11*) preemptively highlighted vulnerabilities in the U.S.' national defense early in President George W. Bush's administration. Following the attack, the nation's political and public will uniformly aligned in the call to identify gaps in our security and national defense which made such horrendous events possible. While common sense after the fact would lead one to believe that this would assist in securing the national critical infrastructure, it did so in a way that retarded the efforts initiated under President Clinton. Unfortunately, 9/11 focused the national will myopically toward the Global War on Terrorism and discounted the likelihood of terrorists using cyber as their primary means of affecting the physical world. As such, the discussion of cyber threats, as introduced in Executive Order No. 13,010, essentially fell to the way-side in lieu of the desire to identify, interdict and disrupt physical attacks. Quite possibly the largest reaction, to the 9/11 attacks, was the establishment of the U.S. Department of Homeland Security and

subsequent absorption/subordination of the Federal Emergency Management Agency (FEMA) (Executive Order No. 13,228, 2001; Homeland Security Act of 2002, 2002, sect. 101(a)).

A major part of the driven effort to identify gaps in national security by understanding the gaps exploited by the 9/11 terrorists was entrusted to the National Commission on Terrorist Attacks Upon the United States *(9/11 Commission)*, which produced a report—Final Report of the National Commission on Terrorist Attacks Upon the United States *(The 9/11 Commission Report)*—for the U.S. Congress and subsequently the U.S. public. It is incorrect to believe that this report was generated quickly or in sufficient time to mollify an incensed U.S. public. In fact, the 9/11 Commission was not even formed until November 2002, over 14 months after the terror event. The 9/11 Commission Report was officially released July 22, 2004, after approximately 20 months of investigation, research and analysis. This is significant as, during that time lag, both President Bush's administration and the U.S. Congress drafted and released numerous key documents which directly addressed a unified national response to domestic national defense breaches (e.g., Executive Order No. 13,231, Homeland Security Act of 2002, Homeland Security Presidential Directive 5, Homeland Security Presidential Directive 7, and Homeland Security Presidential Directive 8).

a. Executive Order No. 13,228–Establishing the Office of Homeland Security and the Homeland Security Council (2001)

Released under a month from the horrific 9/11 terror attacks, on October 08, 2001, Executive Order No. 13,228, established the Office of Homeland Security and the Homeland Security Council.

As this was a reflexive action to the lack of coordinated efforts of responders to the 9/11 attacks, the mission and function, as described in the EO, dictate that the Office of Homeland Security "… coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States" (Executive Order No. 13,228, 2001, sect. 3). Executive Order No. 13,228, in a paragraph titled *National Strategy*, expressly directs that the Office of

Homeland Security "… work with executive departments and agencies, State and local governments, and private entities to ensure the adequacy of the national strategy … from terrorist threats or attacks within the United States and shall periodically review and coordinate revisions to that strategy as necessary" (Executive Order No. 13,228, 2001, sect. 3(a)). This is significant as it highlights the continuation of the unity of effort strategy previously imposed, but also allows the Office of Homeland Security the latitude to perform a reassessment and proposes a different national strategy.

Although provided with a wide mandate initially, Executive Order No. 13,228, in a paragraph titled *Protection*, expressly directs that the Office of Homeland Security shall coordinate efforts to "… protect the United States [sic] and its critical infrastructure" and to "…coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack" (Executive Order No. 13,228, 2001, sect. 3(e)). The specific verbiage in Section 3(e) is vital; this language is the basis for an on-going discussion with regard to the deconfliction of roles and responsibilities since the Office of Homeland Security is mandated to *protect* the nation, while the DoD mandate remains to *defend* the nation.

b. Executive Order No. 13,231–Critical Infrastructure Protection in the Information Age (2001)

Enacted within five weeks of the historic 9/11 terror attacks, on October 16, 2001, Executive Order No. 13,231, titled *Critical Infrastructure Protection in the Information Age*, was signed and released. Under this EO, President Bush established the President's Critical Infrastructure Protection Board (PCIPB) and specifically addressed the interdependent information systems integrated in CI (Executive Order No. 13,231, 2001, sect. 2). This EO also designated the Chair of the PCIPB as the *Special Advisor to the President for Cyberspace Security* (Executive Order No. 13,231, 2001, sect. 7).

To its credit, the PCIPB developed and released the National Strategy to Secure Cyberspace, in February 2003, identifying 24 strategic goals and listing 47 specific recommendations (National Strategy to Secure Cyberspace, 2003). As the nation's open and technologically complex society includes a wide array of CI/KR that

are potential terrorist targets, the PCIPB released the strategy in draft form in September 2002 for public comment and feedback (National Strategy to Secure Cyberspace, 2003, p. 2). This is significant as a majority of the CI are owned and operated by the private sector and State or local governments.

This EO clearly carries the theme started by President Clinton, but is the last such document to emerge with such a direct focus, which highlights the shift from hardening cyber integrated infrastructure to physical protection under DHS.

Interestingly enough, this is the document which delegated security responsibilities of the *Executive Branch Information Systems* to the Director of the Office of Management and Budget (OMB) and security responsibilities of *National Security Information Systems* to the Secretary of Defense and Director of Central Intelligence (Executive Order No. 13,231, 2001, sect. 4). It also coincides with the passing of the Critical Infrastructures Protection Act of 2001, which provides the U.S. policy with respect to CIP (42 U.S.C. 5195c, sect. c(1)).

c. Homeland Security Act of 2002

As early as 2002, Public Law No. 107–296 (more commonly known as the Homeland Security Act of 2002) assigned the DHS as the focal point for the security of cyberspace including: analysis; warning; information sharing; vulnerability reduction; mitigation efforts; and recovery efforts for public and private critical infrastructure and information systems (U.S. Government Accountability Office Testimony 11–865T, 2011). This document is significant as it formally and legally reaffirms FEMA, in its new position under DHS, as the lead agency for the Federal Response Plan (FRP) and thus the lead for responding to cyber threats (Homeland Security Act of 2002, 2002, sect. 507(b)). The FRP was established via Executive Order No. 12,148 and Executive Order No. 12,656 (Homeland Security Act of 2002, 2002, sect. 507(b)).

d. Homeland Security Presidential Directive 5 (2003)

Released February 28, 2003, Homeland Security Presidential Directive 5 (HSPD-5), *Directive on Management of Domestic Incidents,* directed the development

and administration of the National Incident Management System (Homeland Security Presidential Directive 5, 2003, para. 15). HSPD-5 also required the DHS to establish a framework for continuous coordination to provide strategic direction for, and oversight of, the *National Incident Management System* (NIMS) (Homeland Security Presidential Directive 5, 2003, para. 17.b). This framework was later released in December 2004 as the National Response Plan. It one of the first national plans to take cyber into account, by means of an annex identified as the Cyber Incident Annex. This annex established procedures for a "… multidisciplinary, broad-based approach to prepare for, remediate, and recover from catastrophic cyber events impacting critical national processes and the national economy" (National Response Plan, 2004, p. xiii).

e. Homeland Security Presidential Directive 7 (2003)

Released in 2003, the Homeland Security Presidential Directive 7 (HSPD-7) "… establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks" (Homeland Security Presidential Directive 7, 2003, p. 1). The directive expanded the definition of critical infrastructure as previously defined in the Critical Infrastructures Protection Act of 2001. Reverting back to much of President Clinton's definition, this directive defines CI as the physical and virtual systems that are "… so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety."

Unique in this document though is the specific reference to what will later be identified as critical sectors, but was then broken down into separate CI and KR categories, as built upon from the list provided in PDD-63 (1998). In paragraph (15), the document lists six CI sectors as "… information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping" (Homeland Security Presidential Directive 7, 2003, p. 4). Immediately following, the document lists three KR as dams, government facilities, and commercial

facilities (Homeland Security Presidential Directive 7, 2003, p. 4). Building on these, but assigning them to other federal agencies, a later paragraph additionally lists: agriculture; food; healthcare; water; energy; banking and finance; national monuments and icons; and the Defense Industrial Base (DIB) as eight additional CI sectors (Homeland Security Presidential Directive 7, 2003, p. 5). These distinctive lists, totaling 17 CI/KR sectors, are later refined again to create the 18 sectors listed in the National Infrastructure Protection Plan (NIPP) (National Disaster Recovery Framework, 2011, p. 58).

Significantly, HSPD-7 reaffirms the Homeland Security Act of 2002 direction in that DHS "… will continue to maintain an organization to serve as a focal point for the security of cyberspace … [which] includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems" (Homeland Security Presidential Directive 7, 2003, para. 16).

f. Homeland Security Presidential Directive 8 (2003)

Released December 17, 2003, Homeland Security Presidential Directive 8 (HSPD-8), *Directive on National Preparedness*, augments HSPD-5 by directing the Secretary of Homeland Security to "… develop a national domestic all-hazards preparedness goal" (Homeland Security Presidential Directive 8, 2003, para. 5). As stated in the document, the term *all-hazards preparedness* refers to preparedness for domestic terrorist attacks, major disasters, and other emergencies. To achieve the goal, the Secretary of Homeland Security was directed to attempt standardization of training, equipment, and funding awards for first responders, to the extent possible and allowable by law (Homeland Security Presidential Directive 8, 2003). Although developed at the time, the national domestic all-hazards preparedness goal, as directed in HSPD-8, has since been replaced, as directed in Presidential Policy Directive 8 (PPD-8), released in September 2011.

g. The 9/11 Commission Report (2004)

Released July 22, 2004, the Final Report of the National Commission on Terrorist Attacks Upon the United States *(The 9/11 Commission Report*), reported the

findings of a commission mandated to investigate "… facts and circumstances relating to the terrorist attacks of September 11, 2001." The commission broke this down into two very basic questions: (1) how were the terrorist attacks on 9/11 allowed to occur unmitigated, and (2) what changes could be implemented to avoid a reoccurrence (National Commission on Terrorist Attacks Upon the United States, 2004, p. xv)? In addressing the second question, the 9/11 Commission made the following recommendation:

> Recommendation: Emergency response agencies nationwide should adopt the Incident Command System (ICS).When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command. Both are proven frameworks for emergency response. We strongly support the decision that federal homeland security funding will be contingent, as of October 1, 2004, upon the adoption and regular use of ICS and unified command procedures. In the future, the Department of Homeland Security should consider making funding contingent on aggressive and realistic training in accordance with ICS and unified command procedures. (National Commission on Terrorist Attacks Upon the United States, 2004, p. 397)

Although speculative, it is possible that the delay of the 9/11 Commission report's release doomed some of their key findings and recommendations, since President Bush's administration was moved by public outcry to move forward in an immediate and public reorganization, as seen by the Homeland Security Act of 2002. Regardless, the above recommendation clearly suggests a unified command when multiple agencies or jurisdictions are involved, but it also limits the recommendation to response functions and training to that goal.

Oddly enough, following their recommendation of a unified command, the 9/11 Commission then dedicated an entire chapter on to how to reorganize the government. Four of the five section titles in that chapter begin with the words *Unity of Effort* (National Commission on Terrorist Attacks Upon the United States, 2004, p. 400–419). Obviously, already discarding the proposal of a unified command, the 9/11 Commission asked, and then answered, which agency is responsible for national domestic defense? They came to a conclusion and stated in the 9/11 Commission Report that "… national defense at home is the responsibility, first, of the Department of Defense

and, second, of the Department of Homeland Security," with a follow-on caveat that they have clear delineations of responsibility and authority (National Commission on Terrorist Attacks Upon the United States, 2004, p. 427).

To address the responsibilities of the DHS, the 9/11 Commission recommended that they should "… regularly assess the types of threats the country faces to determine (a) the adequacy of the government's plans—and the progress against those plans—to protect America's critical infrastructure and (b) the readiness of the government to respond to the threats that the United States might face" (National Commission on Terrorist Attacks Upon the United States, 2004, p. 428). This recommendation may look familiar as it was previously addressed in HSPD-5, HSPD-7, and HSPD-8 which were released during the compilation of the 9/11 Commission's findings.

h. Homeland Security Presidential Directive 8 Annex 1 (2007)

Augmenting guidance found in HSPD-8 and the National Strategy for Homeland Security (2007), HSPD-8 Annex 1 was released December 4, 2007 and added additional requirements to HSPD-8 and then amended both HSPD-5 and HSPD-8 in an effort to establish conformity. Specifically, HSPD-8 Annex 1 established the requirement for the Secretary of Homeland Security to establish a standardized comprehensive approach to national planning, termed the Integrated Planning System (Homeland Security Presidential Directive 8 Annex 1, 2007, para. 33). More importantly though, this document directed the development of *National Planning Scenarios* using a risk-based analysis model, "… intended to focus planning efforts on the most likely or most dangerous threats to the homeland" (Homeland Security Presidential Directive 8 Annex 1, 2007, para. 34). These National Planning Scenarios are required to:

- have a strategic guidance statement developed by the Secretary of Homeland Security;
- have a strategic plan developed in consultation with other Federal agencies within 90 days of the strategic guidance statement being issued;
- have a concept of operations plan (CONPLAN) developed within 180 days of a strategic plan being approved;

- have an operations plan (OPLAN) developed within 120 days of CONPLAN approval;
- be included in budgetary submissions (for planning and execution) by affected Federal agencies to the Office of Management and Budget; and
- be updated no less frequently than on a biennial basis.

6. President Barrack H. Obama's Administrations

According to the 29th U.S. Deputy Secretary of Defense, William J. Lynn (III): following the "… most significant breach of U.S. military computers ever" in 2008, via malicious code injection through a foreign purchased flash drive, "… the Pentagon … formally recognized cyberspace as a new domain of warfare" (Lynn, 2010, p. 101). As such, the "… Pentagon's operation to counter the attack, known as Operation Buckshot Yankee, marked a turning point in U.S. cyberdefense strategy" (Lynn, 2010, p. 97).

Inheriting this chaotic environment, within a month of President Barrack H. Obama's inauguration, his administration called for the now anticipated review of the nation's strategy to protect critical infrastructure and key resources from the cyber threat.

The below quote is from the Assistant to the President for Counterterrorism and Homeland Security John Brennan, as captured in a White House press statement publically released on February 09, 2009 and is one of the many documents/statements released wherein officials wrestle with the amorphous topic of cyber and its interdisciplinary integrative nature (Greenwald, 2010, p. 41).

> The national security and economic health of the United States depend on the security, stability, and integrity of our Nation's cyberspace, both in the public and private sectors. The President is confident that we can protect our nation's critical cyber infrastructure while at the same time adhering to the rule of law and safeguarding privacy rights and civil liberties. (White House Press Office, 2009)

a. Cyberspace Policy Review (2009)

The aforementioned White House press statement, released February 9, 2009, also publically announced that President Barack H. Obama directed his National

Security and Homeland Security Advisors to conduct a 60-day interagency review to develop a strategic framework to ensure that U.S. government cyber security initiatives were appropriately integrated, resourced and coordinated with Congress and the private sector. The subsequent findings of the 60-day review, titled *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, were released 110 days later on May 29, 2009 (Greenwald, 2010, p. 41).

b. Presidential Policy Directive 8–National Preparedness (2011)

Signed by President Obama on March 30, 2011, the DHS/FEMA coordinated the input for, and compilation of, the multi-agency generated PPD-8 as a means to update the authorities necessary to address the national preparedness system as required in the Post-Katrina Act of 2006; Subtitle C (Lindsay, 2012, p. 4). This document is a lodestone document; PPD-8 drives the majority of the national preparedness documents and procedures currently in effect, or in progress of generation, today. Explicitly pointed out in the first paragraph though is the unity of effort approach as the directive is "… intended to galvanize … an integrated, all-of-Nation [sic], capabilities-based approach to preparedness" (Presidential Policy Directive 8, 2011, p. 1).

This directive explicitly "… replaces Homeland Security Presidential Directive (HSPD)-8 (National Preparedness), issued December 17, 2003, and HSPD-8 Annex I (National Planning), issued December 4, 2007, which were rescinded" (Presidential Policy Directive 8, 2011). On closer inspection, this document orders the exact same approach directed in HSPD-5, HSPD-8 and HSPD-8 Annex 1, as it also required the generation of a national preparedness goal and standardized framework(s) to manage the NIMS. It does uniquely identify though that the strategy employed will be an all-of-nation approach vice whole-of-government or federal approach. This shift in terminology is significant and is the topic of discussion later in this thesis. It also directs the genesis and submission of a *National Preparedness Goal* and *National Planning Framework* by which to achieve the goal.

(1) National Preparedness Goal

The current national preparedness goal generated in response to PPD-8, and provided via the FEMA website, is: "A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk" (National Preparedness Goal, 2011, p. 1).

(2) National Planning Framework

To address the requirements of standardized frameworks, and in an effort to implement the structure necessary to achieve this goal, PPD-8 breaks the National Preparedness System down into five mission areas, each one requiring a blueprint referred to as a National Planning Framework. The five preparedness mission areas are more thoroughly addressed in the next chapter, as it discusses current implementation vice policy.

c. Presidential Policy Directive 20 (2012)

Signed October 26, 2012, and released November 2012, the classification of the PPD-20 precludes open discussion at this level and so is noted solely for posterity.

d. Executive Order No. 13,636–Improving Critical Infrastructure Cybersecurity (2013)

Signed on February 12, 2013, President Obama released Executive Order No. 13,636 which directs federal agencies to develop voluntary cybersecurity standards for critical parts of the private sector and to consider proposing new mandates where possible under existing law. Incorporating many points from the numerous cyber bills that failed to be passed in both houses of the U.S. Congress in the most recent session, this EO requires federal agencies to produce unclassified reports of threats to U.S. companies and to share them in a timely manner with the private-sector (Executive Order No. 13,636, 2013, sect. 4(a)). Also, reiterated in the EO is the call for voluntary disclosure of cyber-related incidents and threats detected by the private sector with the federal government through established relationships, such as the via the DHS National Cybersecurity and Communications Integration Center (NCCIC). This bi-directional information sharing initiative is to be augmented by a national cyber framework by which

CI of the national infrastructure is monitored and assessed, thus increasing visibility of the cyber health of the nation's CI/KR.

D. CHAPTER SUMMARY

As documented above, although concerns about the proper organization of federal responses to national security threats has been a consistent issue across many presidential administrations, it appears that crisis is required to galvanize public and private will to question preparedness. As described above, it was not until a series of catastrophic natural disasters in the late '80s and early '90s and the terror attacks perpetrated on U.S. soil that intense public criticism of the U.S.' federal response mechanism prompted investigation into the U.S.' plans and efforts surrounding disaster response (U.S. Government Accountability Office Report No. GOA/RCED-93–186, 1993, p. 1). As shown, much of the previous work on proactive national federal strategy to respond to *Incidents of National Significance* has been generated by the Executive Branch of the U.S. government in the form of various Executive Orders, Presidential Decision Directives, Homeland Security Presidential Directives, and Presidential Policy Directives. These key references, spanning about thirty-five years, have been created by multiple administrations with differing views and motivations. Although starting out generally addressing the federal response plans surrounding emergencies and disasters thirty five years ago, in the last 17 years the national focus has shifted with the newest threat: cyber. During this time, three separate U.S. presidents initiated a strategy assessment with respect to addressing cyber vulnerabilities of the national CI/KR.

Prompted by a domestic act of terrorism, President Clinton's administration directed an investigation of CI vulnerabilities in PDD-39 (1995) and subsequently identified the critical vulnerability created by interdependent and cyber-supported infrastructures in the release of Executive Order No. 13,010 (1996). As such, President Clinton directed the creation of the President's Commission on Critical Infrastructure Protection (PCCIP) to conduct an analysis of CI in order to protect them and maintain assurance of their continued operation in times of crisis. Following the receipt of PCCIP's report, Critical Foundations, President Clinton released PDD-63 which

implements a personalized version of the unity of effort strategy by breaking the critical infrastructure into sectors and parsing out lead roles to Federal agencies.

The terror attacks on 9/11, at the beginning of President Bush's administration, preemptively highlighted vulnerabilities in the U.S. national defense of CI/KR. As such, through the release of Executive Orders No. 13,228 and 13,231, just weeks after the terror attack, President Bush directed the formation of both the DHS and PCIPB. Following the immediate response and formation of those bodies, the creation of the 9/11 Commission was directed to conduct an analysis of CI and agency roles using experts and insiders. Understandingly, his administration was required to act immediately though, prior to the compilation of findings. Therefore, even before submission of findings by the congressionally directed commission, the Homeland Security Act of 2002, HSPD-5, HSPD-7, and HSPD-8 were released in the span of 13 months and highlighted the *whole of government* approach, which equates to the unity of effort strategy. Following the receipt of the 9/11 Commission's report, Final Report of the National Commission on Terrorist Attacks Upon the United States (2004), President Bush released HSPD-8 Annex 1 which simply further implements his administration's reflexive unity of effort strategy established in the previously released documents and essentially ignored the recommendation citing the unity of command strategy.

President Obama's administration identified the critical vulnerability inherent in the nation's cyberspace early in his first term following the "… most significant breach of U.S. military computers ever" in 2008 (Lynn, 2010, p. 97). As such, he directed his National Security and Homeland Security Advisors to conduct a Cyberspace Policy Review in order to develop a strategic framework with which to ensure integration and coordination with the U.S. Congress and the private sector. Following the receipt of the report from the Cyberspace Policy Review, President Obama released PPD-8, PPD-20 and Executive Order No. 13,656 which implements yet a third personalized version of the 'Unity of Effort' strategy.

Documented above, from the last three U.S. presidents, is that all of the efforts from 1996 to present to address protecting national CI from cyber threats seem circular in

nature as each new presidential administration in the last 17 years: (1) identifies a critical vulnerability in the national defense of critical infrastructure, (2) creates a committee of experts and insiders to research and evaluate issues, and (3) then implements a personalized unity of effort strategy.

The following chapter outlines the current unity of effort implementation via the national preparedness system, as directed by PPD-8, and then is followed by a chapter which lays out the authorities and efforts of the agencies covered by the relevant U.S. Codes.

THIS PAGE INTENTIONALLY LEFT BLANK

III. UNITY OF EFFORT–CURRENT IMPLEMENTATION

According to the presidentially directed Cyberspace Policy Review released May 29, 2009, securing cyberspace "… transcends the jurisdictional purview of individual departments and agencies because … no single agency has a broad enough perspective or authority to match the sweep of the problem" (Cyberspace Policy Review, 2009, p. iv). Subsequently, President Barrack H. Obama issued PPD-8 on May 30, 2011 which directed "… the development of a national preparedness goal that identifies the core capabilities necessary for preparedness and a national preparedness system to guide activities that will enable the Nation to achieve the goal" (Presidential Policy Directive 8, 2011, p. 1).

A. NATIONAL PREPAREDNESS GOAL

The National Preparedness Goal is a document generated in response to PPD-8 and released as a First Edition in September 2011. The document identifies the core capabilities needed to deal with significant risks to the Nation and was developed to "… reflect the policy direction outlined in the National Security Strategy (May 2010)" (Presidential Policy Directive 8, 2011, p. 2).

1. National Preparedness Goal

The actual preparedness goal, as listed on page one of the document, is also provided on the FEMA website as: "A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk" (National Preparedness Goal, 2011, p. 1).

2. Mission Areas

To aid in building the requisite capabilities needed to achieve the national preparedness goal, five mission areas, shown in Figure 1, were identified: prevention, protection, mitigation, response, and recovery (National Preparedness Goal, 2011, p. 2).

These mission areas are intended as overarching categories which are comprised of core capabilities.

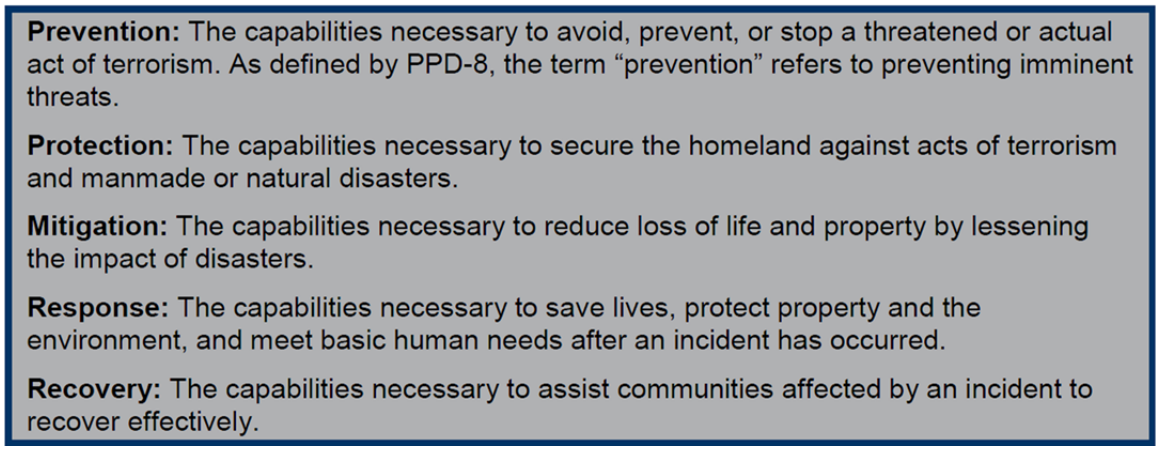

Figure 1. National Preparedness Mission Areas (From National Prevention Framework, 2013, p. 1)

3. Core Capabilities

Additionally, the National Preparedness Goal lists 31 *core capabilities*, subordinated under the five mission areas, deemed necessary to achieve the stated national preparedness goal. Graphically depicted in Table 1 is the alignment of the core capabilities under the five national preparedness mission areas (National Preparedness Goal, 2011, p. 2). One of the core capabilities, as noted in Table 1, is Cybersecurity subordinated under the Protection mission area. Although the majority of the core capabilities have a cyber aspect, the discussion that follows will focus on the highlighted ones in Table 1. In review of the individual documents, these seem to more directly support cybersecurity of the CI/KR subset. Because the documents describe the other core capabilities in a broader holistic view, the focus is on the highlighted entries.

Prevention	Protection	Mitigation	Response	Recovery
Planning				
Public Information and Warning				
Operational Coordination				
Forensics and Attribution	Access Control and Identity Verification	Community Resilience	Critical Transportation	Economic Recovery
Intelligence and Information Sharing	Cybersecurity	Long-term Vulnerability Reduction	Environmental Response/Health and Safety	Health and Social Services
Interdiction and Disruption	Intelligence and Information Sharing	Risk and Disaster Resilience Assessment	Fatality Management Services	Housing
Screening, Search, and Detection	Interdiction and Disruption	Threats and Hazard Identification	Infrastructure Systems	Infrastructure Systems
	Physical Protective Measures		Mass Care Services	Natural and Cultural Resources
	Risk Management for Protection Programs and Activities		Mass Search and Rescue Operations	
	Screening, Search, and Detection		On-scene Security and Protection	
	Supply Chain Integrity and Security		Operational Communications	
			Public and Private Services and Resources	
			Public Health and Medical Services	
			Situational Assessment	

Table 1. Core Capabilities by Mission Area (From National Preparedness Goal, 2011, Table 1)

B. NATIONAL PREPAREDNESS SYSTEM

As directed by the guidance provided in PPD-8, the National Preparedness System was released by Department of Homeland Security (DHS) in November 2011 as a 10-page document. Still in use today, the underlying purpose of the document is to outline the phases by which the Nation will "… employ to build, sustain, and deliver those core capabilities in order to achieve the goal of a secure and resilient Nation" (National Preparedness System, 2011, p. 1). This document identifies and describes six components of the National Preparedness System, which are listed as: identifying and assessing risk, estimating capabilities required, building or sustaining required capabilities, planning to deliver required capabilities, validating and monitoring

capability progress, and reviewing and updating efforts for continuous improvement (National Preparedness System, 2011, p. 1).

1. Identifying and Assessing Risk

As the first component to a six-step cyclical process, the first step relies on the creation and execution of risk assessments—Threat and Hazard Identification and Risk Assessments (THIRA), Strategic National Risk Assessments (SNRA), and specialized risk assessments (National Preparedness System, 2011, p. 2). Below the national level, THIRA guidance is being developed and planned to "… provide a common, consistent approach for identifying and assessing risks and associated impacts," enabling improved integration of threats into the overall risk assessment process (National Preparedness System, 2011, p. 2). The national level will primarily rely on the SNRA and specialized risk assessments to identify the greatest risks to the nation (National Preparedness System, 2011, p. 2).

a. Strategic National Risk Assessment

The SNRA was released in December 2011 in both classified (full version) and unclassified (sanitized) documents. For discussion, the unclassified version of the SNRA was used in this paper, as it highlights the "… evaluated … risk from known threats and hazards that have the potential to significantly impact the Nation's homeland security" (Strategic National Risk Assessment, 2011, p. 1). Of the identified ten national-level threats generated from an adversary, as depicted in Table 2, two of those utilize the cyber domain, but set clearly delineated thresholds for effects of cyber-attacks which in and of themselves are difficult to assess and definitively quantify in monetary values.

Threat/ Hazard Group	Threat/Hazard Type	National-level Event Description
Adversarial/ Human-Caused	Aircraft as a Weapon	A hostile non-state actor(s) crashes a commercial or general aviation aircraft into a physical target within the U.S.
	Armed Assault	A hostile non-state actor(s) uses assault tactics to conduct strikes on vulnerable target(s) within the U.S. resulting in at least one fatality or injury
	Biological Terrorism Attack (non-food)	A hostile non-state actor(s) acquires, weaponizes, and releases a biological agent against an outdoor, indoor, or water target, directed at a concentration of people within the U.S.
	Chemical/Biological Food Contamination Terrorism Attack	A hostile non-state actor(s) acquires, weaponizes, and disperses a biological or chemical agent into food supplies within the U.S. supply chain
	Chemical Terrorism Attack (non-food)	A hostile non-state actor(s) acquires, weaponizes, and releases a chemical agent against an outdoor, indoor, or water target, directed at a concentration of people using an aerosol, ingestion, or dermal route of exposure
	Cyber Attack against Data	A cyber attack which seriously compromises the integrity or availability of data (the information contained in a computer system) or data processes resulting in economic losses of a Billion dollars or greater
	Cyber Attack against Physical Infrastructure	An incident in which a cyber attack is used as a vector to achieve effects which are "beyond the computer" (i.e., kinetic or other effects) resulting in one fatality or greater or economic losses of $100 Million or greater
	Explosives Terrorism Attack	A hostile non-state actor(s) deploys a man-portable improvised explosive device (IED), Vehicle-borne IED, or Vessel IED in the U.S. against a concentration of people, and/or structures such as critical commercial or government facilities, transportation targets, or critical infrastructure sites, etc., resulting in at least one fatality or injury
	Nuclear Terrorism Attack	A hostile non-state actor(s) acquires an improvised nuclear weapon through manufacture from fissile material, purchase, or theft and detonates it within a major U.S. population center
	Radiological Terrorism Attack	A hostile non-state actor(s) acquires radiological materials and disperses them through explosive or other means (e.g., a radiological dispersal device or RDD) or creates a radiation exposure device (RED)

Table 2. Strategic National Risk Assessment–Adversarial Risks
(From Strategic National Risk Assessment, 2011, Table 1)

The overall utility of the identification of the cyber threat in the SNRA is useful, but precluded by the clearly defined monetary threshold to meet the poorly written national-level event criteria. Specifically, the chosen wording is likely over-simplified in addressing the cyber threat as it exists in today's world, whether intentional or not. Two keys issues with the description: (1) it omits addressing confidentiality, as a key

component of cybersecurity; and (2) it omits accounting for coordinated efforts resulting in multiple attacks.

The description for a cyber-attack on data, listed in Table 2, takes into account only two of the three aspects of the Cybersecurity triad—integrity and availability. As such, this description is limited to denial of service attacks and modification, deletion, and injection of data. It therefore omits the third aspect of Cybersecurity—confidentiality. This is notable as the May 2013 NIST Glossary of Key Information Security Terms cites the Committee on National Security Systems Instruction 4009, titled National Information Assurance (IA) Glossary, when defining cyber-attack, which includes "… stealing controlled information" (Glossary of Key Information Security Terms, 2013, p. 57; Committee on National Security Systems Instruction 4009, 2010, p. 22). This omission, however, is therefore likely intended to keep the INS thresholds focused on keeping the national CI/KR up and running; theft of information does not have the same impact, at least in the near term.

Additionally, both descriptions highlighted above suggest a single cyber-attack (or incident) versus a coordinated set of attacks or campaign by a group or individual. In today's world, following the release of Cybersecurity reports such as the Mandiant APT1 report (released in 2013) highlighting dedicated coordinated cyber-attacks to undermine proprietary information important to the U.S. economy (APT1: Exposing One of China's Cyber Espionage Units, 2013). To further highlight this deficiency, Chairman Mike Rogers of the U.S. House of Representative Permanent Select Committee on Intelligence stated on February 14, 2013 in an open congressional hearing that "… China's pervasive and growing economic cyber espionage campaign against American companies … has grown exponentially both in terms of its volume and the damage it is doing to our nation's economic future … because some of our most innovative ideas and sensitive information are being brazenly stolen by these cyber-attacks" (Rogers, 2013). Although Chairman Rogers' use of the term cyber-attack to refer to incidents of espionage, others use the term cyber-attack solely in the sense of disruption or denial. This distinction remains a significant topic of on-going diplomatic

and academic debates as the cyber lexicon is not standardized. This highlights one such example of the necessity for standardized lexicon for the cyber realm.

2. Estimating Capabilities Required

The National Preparedness System guidance for this step directs the use of the risk assessment results to determine the required types and levels of capabilities required to achieve outcome(s) for each mission area (National Preparedness System, 2011, pp. 2–3). The requirements analysis is crucial to proper risk assessment and allocation of resources.

3. Building or Sustaining Required Capabilities

The National Preparedness System guidance for this step directs the creation of the required capabilities after an initial assessment of current ones, based on risk mitigation of highest priority first (National Preparedness System, 2011, p. 3). The sustainment of core capabilities are stated to be maintained through training and education: the *National Training & Education System* (NTES) will support the National Preparedness System by integration of government training facilities, academic institutions, and private organizations (National Preparedness System, 2011, p. 3). Aiding this objective as recently as March 2013, the National Institute of Standards and Technology (NIST), working with federal government agencies, public and private experts and organizations, and industry partners, via the NIST National Initiative for Cybersecurity Education provided a document to address the common understanding of cybersecurity work: National Cybersecurity Workforce Framework (National Cybersecurity Workforce Framework, 2013).

4. Planning to Deliver Required Capabilities

Finally delivering tangible and clearly directed guidance, this section of the document introduces the National Planning System, as it is intended to support the delivery of the core capabilities identified in the National Preparedness Goal (National Preparedness System, 2011, p. 4). This is significant as the National Planning System lays out the guidance for a collaboratively developed set of coordinated National

Frameworks, developed to focus the whole of government on how they should prepare to "… deliver capabilities in each of the five mission areas" (National Preparedness System, 2011, p. 4). Therefore, it is in this step of the National Preparedness System that the plans are being made to address the gaps in required capabilities and current ones through the National Frameworks of the National Planning System.

5. Validating and Monitoring Capability Progress

The progress toward the National Preparedness Goal fulfillment is done through "… exercises, remedial action management programs, and assessments" (National Preparedness System, 2011, p. 5). This section is highly dependent on internal motivation at the organizational level and lacks significant oversight or responsibility assignment. For example, the National Preparedness System identifies the *comprehensive assessment system* (CAS) as a primary means of monitoring and justifies CAS use, but then omits the identification of the organization responsible, method of dissemination, and actions available for remediation (National Preparedness System, 2011, p. 5).

6. Reviewing and Updating Efforts

This section simply identifies the need for periodic reassessments of the core capabilities, but is otherwise unhelpful (National Preparedness System, 2011, p. 6).

7. Conclusion

Overall, this high-level document, encompassing everything from chemical spills to cyber-attacks, and therefore does not address specific processes or baseline any of the core capabilities provided in the National Preparedness Goal. A specific exception would be the direction to complete SNRA's and direction to revisit them periodically, which is worked into the National Planning System. Otherwise, this high-level document (National Preparedness System) highlights the nascent efforts of the federal response by focusing on six areas of common interest.

The extension of the National Preparedness Goal, and alignment of the 31 core capabilities under the five mission areas, is more clearly shown in the National Planning System.

C. NATIONAL PLANNING SYSTEM

To address the requirements of standardized frameworks for each of the five national preparedness mission areas, and in an effort to implement the structure necessary to achieve this goal, PPD-8 breaks the National Preparedness System down into five corresponding blueprints, referred to as a National Planning Frameworks. These frameworks together are termed the National Planning System and are designed to provide a "… detailed concept of operations; a description of critical tasks and responsibilities; detailed resource, personnel, and sourcing requirements; and specific provisions for the delivery of capabilities under each Framework by the Federal Government" (National Preparedness System, 2011, p. 4). They also address how the federal government will support state, territorial, tribal, and local plans and "… the frameworks are used to designate roles and responsibilities …" of the 33 core capabilities identified in the National Preparedness Goal (National Preparedness System, 2011, p. 4). The five preparedness mission areas of the National Planning System, addressed in PPD-8, are listed below as *prevention*, *protection*, *mitigation*, *response*, and *recovery*. Covered below in more detail, three of the mandated frameworks were published in May 2013; one framework remains unpublished; and the final framework is operating from a legacy document dated from September 2011, which states that it will be updated after the initial four frameworks are published and released.

1. National Prevention Framework

The National Prevention Framework, released in May 2013, addresses the process of preparing the nation to prevent an imminent terrorist attack, as the other frameworks more fully account for natural disaster, hazards and incidents (Lindsay, 2012, pp. 4–5). Specifically, the National Prevention Framework "… sets the strategy and doctrine for building, sustaining, and delivering the core capabilities for Prevention identified in the National Preparedness Goal" (National Prevention Framework, 2013, p. 1). More importantly, it assigns roles and responsibilities to the seven associated core capabilities, two of which are directly pertinent to the cyber threat—Intelligence and Information Sharing, and Interdiction and Disruption.

a. Intelligence and Information Sharing

Numerous national incidents (e.g., 9/11 and Oklahoma City bombing) point to the fact that "… no single agency, department, or level of government can independently complete a threat picture of all terrorism and national security threats" (National Prevention Framework, 2013, p. 11). As such, cyber events are rarely isolated events and are highly dependent on the isolation of individual networks and compartmentalization of discovered threats.

Thus, in accordance with existing laws, directives, and policies, this core capability relies on the full "… information sharing and analysis of federal agencies; state and major urban area fusion centers; and the intelligence community during times of imminent threat" (National Prevention Framework, 2013, p. 11). To be effective, this means that intelligence collection prioritization and socialization is required across all concerned agencies so that the limited national assets and resources can be appropriately apportioned. This necessity affects law enforcement, the DoD, the DHS and private organizations and is directly applicable to cyber-attacks conducted by terrorist organizations.

b. Interdiction and Disruption

Of the nine critical tasks listed in the National Prevention Framework, the final critical task, under the section titled Interdiction and Disruption, is directly relevant in terms of cyber threats as employed by terrorists: "…strategically deploy assets to interdict, deter or disrupt threats from reaching potential target(s)" (National Prevention Framework, 2013, p. 13).

From a cyber-centric viewpoint, this specific critical task reinforces the EINSTEIN use by DHS and similar systems, such as those employed by the DoD to prevent unauthorized intrusions into the Global Information Grid (GIG). Of note, EINSTEIN, DHS' integrated Intrusion Detection System (IDS)/Intrusion Protection System (IPS) hybrid is discussed at more length in Chapter IV, para. A.3.d(1).

2. National Protection Framework

While not yet published, the National Protection Framework is clearly the most germane document of the National Planning System to the national cyber strategy to protect CI/KR. As shown in Table 1 previously, of the five mission areas, Protection not only has the continuation of both of the previously identified core capabilities, but also has the only directly applicable core capability—Cybersecurity. That fact, coupled with the DHS mandate to protect CI, insinuates that the National Protection Framework will be a lodestone document identifying Cybersecurity roles and responsibilities, once published and released. It is also important to make the distinction that the National Protection Framework is likely to not be as restrictive as the National Prevention Framework, and will therefore encompass more than the singularity of a terrorist use of the cyber domain to attack national CI/KR.

3. National Mitigation Framework

The National Mitigation Framework, released in May 2013, addresses the process of risk management and the selection and implementation of mitigating factors and processes. This mission area is heavily reliant on accurate and updated situational awareness of vulnerabilities, as provided in the SNRAs and special assessments.

Although significant to the overall process, this document offers little other than distinct support for the unity of effort concept in the roles and responsibilities as shown in Table 3. Two of these roles and responsibilities, highlighted in the table, directly tie back to the SNRA which is used to identify the current threats and hazards.

Role/Responsibility	Individuals, Families, and Households	Communities	Nongovernmental Organizations	Private Sector Entities	Local Governments	State, Tribal, Territorial, and Insular Area Governments	Federal Government
Work with the Federal Government to inform the assessment, development, and coordination of mitigation core capabilities.		X	X	X	X	X	
Coordinate the national assessment and report on the progress made within the mitigation core capabilities.							X
Use regulatory authorities and provide funds, incentives, expertise, and leadership to promote the development, implementation, and assessment of mitigation core capabilities. For example, use financial incentives and targeted capital improvement projects to reduce long-term vulnerabilities.					X	X	X
Contribute to the general understanding of risk through the collection, development, analysis, and sharing of information about threats, hazards, and vulnerabilities, as well as through constant evaluation and enhancement of risk assessment methodologies.			X	X	X	X	X
In coordination with other mission areas, develop, fund, and deliver training curricula for preschool, grades K–12, colleges and universities, continuing education, and the whole community to develop proficiency in understanding risks and mitigation.			X	X	X	X	X
Engage with local leaders and planners to share perspectives on localized threats and hazards, vulnerabilities, and priorities for incorporating mitigation into community planning and development, therefore making achieving resilience a part of the community both before and after a disaster.	X	X	X	X	X	X	X
Assess risks and disaster resilience. Maintain awareness of threats, hazards, and vulnerabilities.	X	X	X	X	X	X	X

Table 3. Mitigation Roles and Responsibilities
(From National Mitigation Framework, 2013, Table 1)

Significant to the discussion is that although listed in the table above as having roles and responsibilities, the categories of Individuals, Families and Households; Communities; Nongovernmental Organizations; and Private Sector Entities are in no way compelled by or accountable to the National Preparedness Goal, National Planning System, or National Mitigation Framework. Thus Table 3 is an ideal that relies either on a strong sense of nationalistic pride or broader understanding of the interdependent nature of national CI/KR by otherwise self-serving entities. The only value is for planners to realize that the span of control is beyond that which they can directly affect without significant private-sector buy-in or ownership. This line of thinking returns to the previous argument that the majority of the entities listed are for-profit and affected only by their profitability. Thus, mitigation of risks and hazards as identified in the SNRA may not be fully embraced if it cuts into their holdings or creates ancillary compliance requirements. Post-INS event response is more likely to generate the desired level of cooperation.

4. National Response Framework

The National Response Framework (NRF) pre-dated the National Preparedness System in its first version, released in 2008 to supersede the National Response Plan (NRP). Following the direction of the guidance in PPD-8, the second version, subordinated under the National Preparedness Goal, was published in May 2013.

The NRF, in its updated form, describes "… the principles, roles and responsibilities, and coordinating structures for delivering the core capabilities required to respond to an incident" (National Response Framework, 2013, p. i). As such, it has specific annexes to address specific incidents and explicitly covers emergencies and disasters resulting from cyber intrusions (National Response Framework, 2013, p. 5).

a. Critical Infrastructure and Key Resources Support Annex

Released in January 2008, the CI/KR Support Annex details the roles and responsibilities relative to the National Response Framework (2008, 1st Ed.) (Critical Infrastructure and Key Resources Support Annex, 2008, p. 1). Graphically depicted in Table 4, this annex breaks down the national CI/KR into 17 sectors and assigns Sector-Specific Agencies (SSA) to act as the lead on each. Information sharing internal to the SSAs can be done through many means, but the primary framework continues to be via Information Sharing and Analysis Centers (ISACs), first introduced in PPD-63 (1998) (Critical Infrastructure and Key Resources Support Annex, 2008, p. 3).

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture[20]	Agriculture and Food
Department of Health and Human Services[21]	
Department of Defense[22]	Defense Industrial Base
Department of Energy[23]	Energy
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems[24]
Department of Homeland Security	
Office of Infrastructure Protection	Chemical
	Commercial Facilities
	Dams
	Emergency Services
	Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Communications	Information Technology
	Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration/U.S. Coast Guard[25]	Transportation Systems[26]
Immigration and Customs Enforcement/Federal Protective Service	Government Facilities

Table 4. CI/KR Assignments to Sector-Specific Agencies (From Critical Infrastructure and Key Resources Support Annex, 2008, Table A-1)

Highlighted in Table 4, the DHS Office of Cyber Security and Communications (CS&C) is assigned as the lead SSA for both the Information Technology and Communications CI sectors. This apparent assignment may be misleading, though, when addressing an INS originating from a cyber-threat, as cyber-attacks can have catastrophic consequences and cascading effects into other CI sectors (e.g., Dams, Transportation Systems, and Banking and Finance) (National Mitigation Framework, 2013, p. 6). Inasmuch, cyber-attacks on the national CI/KR will likely be dealt with in the duality in which they exist; DoD will utilize their *defend the nation* mandate to counter, degrade, or disrupt the attack while DHS will exercise their *protect the nation* mandate by leading efforts to respond, mitigate and eventually recover from the damage caused by the attack(s).

5. National Recovery Framework

Pre-dating the release of the National Preparedness System, the DHS recovery efforts are currently coordinated in accordance with the National Disaster Recovery Framework (NDRF), published in September 2011. When the National Recovery Framework is published it will replace the older NDRF. With the acknowledgment that the revised framework will need to be compatible with the other frameworks, the NDRF itself states that it will be revised as the National Preparedness System is further developed and the other preceding frameworks of prevention, protection, mitigation and response frameworks are finished (National Disaster Recovery Framework, 2011, p. 7). Although not yet accomplished, such a revision should ensure that actions listed to be taken in the NDRF are coordinated within the spirit of the other frameworks and appropriately provide the next logical step in the preparedness continuum.

Presumably due to the fact that this is a legacy framework, the NDRF accounts for the core capability of *Infrastructure Systems*, not as a core capability, but rather references it as a *Recovery Support Function* (RSF) (National Disaster Recovery Framework, 2011, p. 37). The RSF correspondingly was assigned a pre-designated coordinating agency to promote communication and collaboration, as well as assigning primary supported agencies.

a. Infrastructure Systems

The DoD U.S. Army Corps of Engineers (USACE) is listed as the coordinating agency for infrastructure systems, with DHS (FEMA and NPPD), DoD/USACE, Department of Energy (DOE), and Department of Transportation (DOT) listed as the primary supported agencies (National Disaster Recovery Framework, 2011, p. 58). Therefore, although DHS has the lead for ensuring the National Preparedness Goal mission area of recovery is properly utilized following an INS, DoD (via USACE) is the actual coordinating agency for addressing the core capability of infrastructure systems. In light of a cyber-attack on those systems, it must be assumed coordinating authority does not equate to sole responsibility, as cyber infrastructure will need to be analyzed for intentional or unintentional parasitic malware by industry and cybersecurity experts.

D. CHAPTER SUMMARY

Although the NIMS covers both of the concepts of multi-agency coordination (unity of effort) and unity of command in the command and management component, the newly formed National Planning System focuses on implementing only the former (National Incident Management System, 2008, p. 48).

To implement the unity of effort approach, the National Preparedness Goal, as reiterated by the National Preparedness System, is implemented through the National Planning System in five mission areas and 31 core capabilities. Although not fully developed and released, the five parallel frameworks tied to the mission areas detail the roles and responsibilities corresponding to core capabilities. More specifically, defending our nation's CI/KR from the cyber threat is a task comprised of many core capabilities, but the key one (Cybersecurity) has not been fully addressed, as the National Protection Framework has yet to be released.

Finally, although addressed in the SNRA, identification of the cyber INS threshold is useful but precluded by: the difficulty in definitively calculating monetarily defined effects post cyber-attack, in order to assess the damage in relation to the significant thresholds to meet the national-level event criteria; and the singularity of the term attack and incident, thus discounting the coordinated campaigns and attacks observed (e.g., Georgia, and 2012–2013 attacks on U.S. Banking and Financial sector) (Hollis, 2011; Perlroth & Sanger, 2013).

Therefore, although significant time and effort has been devoted to capturing the process of implementing the frameworks to build and assess the core capabilities, little in the way of cyber-related roles and capabilities are directly addressed to date. Despite this, many federal agencies continue to operate under standing authorities with the intent to address what they view as their mission in the operational cyber domain. The next chapter addresses some of those authorities as a nascent effort to identify the key agencies and existing authorities.

IV. AUTHORITIES, ROLES, AND EFFORTS

The Critical Infrastructures Protection Act of 2001 states that the official U.S. policy is that "… any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States" (42 U.S.C. 5195c, sect. c(1)).

To achieve this, with applicable statutory authorities already in place, the U.S. previously managed crises through the separate lenses of national defense, law enforcement, and emergency management prior to the initiation of the ongoing policy discussion of homeland security (Painter, 2013, p. 2). The terrorist attacks on September 11, 2001, however, did in fact initiate that discussion through an immediate review of U.S. strategic policies that included a debate over, and the development of, a holistic national domestic defense policy—termed homeland security policy. *The 9/11 Commission Report* specifically recommended that the DHS regularly assess threats to determine the adequacy of the government's plans to protect America's CI and the readiness of the U.S. government to respond (National Commission on Terrorist Attacks, 2004, p. 428). As such, discussion, development, and evolution of domestic policy over the last 12 years have resulted in numerous federal agencies with homeland security responsibilities and funding. For example, multiple Congressional Research Service reports, released early 2013, point out that there are 30 federal agencies that receive annual homeland security funding, excluding the DHS (Painter, 2013, p. 2; Reese, 2013, p. 1; OMB, 2013). Additionally, the Office of Management and Budget (OMB) estimates that 48% of annual homeland security funding is appropriated to these federal agencies, with the DHS receiving approximately 52% (Reese, 2013, p. 1).

It should appear obvious to even the casual observer that, to achieve the stated policy and with so many federal agencies involved, cyberspace functions can and frequently do significantly overlap; cyberspace operations, as outlined in 2009, were executed throughout the multiple federal executive agencies as authorized by U.S. Code (U.S.C.): Title 6 (Domestic Security); Title 10 (Armed Forces); Title 18 (Crime and

Criminal Procedures); Title 44 (Public Printing and Documents); and Title 50 (War and National Defense) responsibilities (Joint Forces Quarterly, 2009). Now four years later the recently released DoD Joint Publication 3–12 (*Cyberspace Operations*), signed on February 5, 2013, attempted to capture the overlap in cyber domain authorities with greater specificity in its Figure III-1, depicted in Table 5. Combined, Table 5, with those authorities created for the protection of national CI/KR, expands the field of research for the protection of national CI/KR from cyber-attacks and intrusions greatly as it now also includes: Title 32 (National Guard); Title 40 (Public Buildings, Properties, and Works); and Title 42 (Public Health and Welfare).

UNITED STATES CODE-BASED AUTHORITIES				
US Code	**Title**	**Key Focus**	**Principal Organization**	**Role in Cyberspace**
Title 6	*Domestic Security*	Homeland security	Department of Homeland Security	Security of US cyberspace
Title 10	*Armed Forces*	National defense	DOD	Secure US interests by conducting military operations in cyberspace
Title 18	*Crimes and Criminal Procedure*	Law enforcement	Department of Justice	Crime prevention, apprehension, and prosecution of criminals operating in cyberspace
Title 32	*National Guard*	Train to perform Title 10, USC missions and perform duties during a state of emergency as declared by the governor of their state	State Army National Guard, State Air National Guard	Domestic consequence management (If activated for federal service, the National Guard is integrated into the Title 10, USC, Armed Forces)
Title 40	*Public Buildings, Property, and Works*	Chief Information Officer roles and responsibilities	All Federal Departments and Agencies	Establish and enforce standards for acquisition and security of information technologies
Title 50	*War and National Defense*	Foreign intelligence and counter-intelligence activities	Intelligence community agencies aligned under the Office of the Director of National Intelligence	Intelligence gathering through cyberspace on foreign intentions, operations, and capabilities

Table 5. United States Code-Based Authorities (From JP 3–12, 2013, Figure III-1)

This chapter will address the primary agencies involved categorized by the authorities under which they maintain a role in the protection of national CI/KR from cyber-attacks and intrusions.

A. U.S. CODE TITLE 6

Title 6 of the U.S. Code is titled Domestic Security and primarily provides the statutory authorities governing the DHS. As such, the remainder of this section will look at DHS authorities, roles and efforts as they relate to cybersecurity and the protection of CI/KR.

As recently as May 16, 2013, in his opening statement for the hearing on "Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities," Chairman of the House of Representative's Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies Patrick Meehan reaffirmed DHS' mandate, from the Homeland Security Act of 2002, as the lead in CI protection.

> While our military protects our nation from foreign adversaries, the security of our critical infrastructure—our economy, our roads and bridges, domestic energy, water and public utility systems—must be a collaborative effort between the private sector, and local, state, and federal government. We need a civilian agency to facilitate this partnership. And that agency is the Department of Homeland Security. (Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities, 2013, p. 2)

1. DHS Authority

DHS originated from the creation of the Office of Homeland Security in the Executive Office of the Presidency, via Executive Order No. 13,228 (2001), which was tasked with the mission "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks" (Executive Order No. 13,228, 2001, sec. 2). The authority of the U.S. president to perform these reorganizations lay in statutory authority in 5 U.S.C. §901-903.

a. Homeland Security Act (2002)

The Homeland Security Act of 2002, Pub. L. 107–296, 116 Stat. 2135 (2002) (6 U.S.C. §101–557), as amended by the Department of Homeland Security Appropriations Act of 2007, Pub. L. 109–295, 120 Stat. 1355 (2006), established the

DHS as an executive department. The DHS was formally established in order to "… consolidate all of the domestic agencies responsible for securing America's borders and national infrastructure, most of which is in private hands" (National Commission on Terrorist Attacks Upon the United States, 2004, p. 428). More specifically, Two key statutory authorities of note are provided to DHS in the Homeland Security Act of 2002 with relation to cybersecurity: protect the nation and to provide analysis and warnings to non-federal entities with respect to critical information systems [cybersecurity] (6 U.S.C. §112; 6 U.S.C. §143). These are covered in more depth later in this chapter.

b. Homeland Security Presidential Directive 23 (2008)

Originally classified when released near the end of President George W. Bush's second term, Homeland Security Presidential Directive 23 (HSPD-23) / National Security Presidential Directive 54 (NSPD-54) were signed in January 8, 2008. According to a 2010 DHS report titled *Computer Network Security and Privacy Protection*, HSPD-23/NSPD-54 (titled *Cyber Security and Monitoring*) formalized the Comprehensive National Cybersecurity Initiative (CNCI), which now "… authorizes DHS, together with OMB, to establish minimum operational standards for Federal Executive Branch civilian networks so that US-CERT can direct the operation and defense of government connections to the Internet" (U.S. Department of Homeland Security, 2010, p. 2).

Combined, NSPD 54/HSPD 23, in conjunction with CIP authorities under the Homeland Security Act of 2002, designate the DHS to coordinate the national cybersecurity effort in the "… prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure availability, integrity, authenticity, confidentiality, and non-repudiation is maintained across cyberspace" (U.S. Department of Homeland Security, 2010, p. 2).

2. DHS Existing Role

As the propensity of U.S. CI/KR are owned by the private sector and state or local governments, it has required the establishment of effective partnerships between the public and private sectors to *protect* these cyber-reliant critical assets from a multitude of

threats, including terrorists, criminals, and hostile nations (Homeland Security Presidential Directive 7, 2003; GAO Testimony 11–865T, 2011).

a. Protect the Nation

Significant distinction must be given to the word protect, as, per the Homeland Security Act of 2002 (sect. 102, para. f.1), it is "… the primary mission of the Department [sic] to protect the American homeland" (6 U.S.C. §112).

With this ominous mission in mind, at cursory read, the DHS is also tasked in the Homeland Security Act of 2002 (sect. 101, para. b.1.F) to protect the economic security of the U.S., which would grant the DHS the necessary leeway to actively pursue entities stealing intellectual property utilizing the cyber domain. A careful read, however, shows this to be an incorrect or rather incomplete interpretation of the law. What is actually stated is that DHS will "… ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland…" (6 U.S.C. §111, sect. 101, para. b.1.F). Thus, it should be understood that DHS has their mandate to protect the U.S., with the additional caveat that DHS pursue their mission while not jeopardizing U.S. economic security through unsustainable expenditures. While sensible at the time of formation, this subparagraph is unnecessary in its current form, but may provide a unique and simple means to modernize DHS authority with respect to today's national vulnerability created through the interdependencies in the cyber domain.

b. Cybersecurity Support to Non-federal Entities

Additionally, the Homeland Security Act of 2002, Pub. L. 107–296, 116 Stat. 2135 (2002) directed that DHS shall—

> (1) as appropriate, provide to State and local government entities, and upon request to private entities that own or operate critical information systems —
>
> > (A) analysis and warnings related to threats to, and vulnerabilities of, critical information systems; and

> (B) in coordination with the Under Secretary for Emergency Preparedness and Response, crisis management support in response to threats to, or attacks on, critical information systems; and
>
> (2) as appropriate, provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems. (6 U.S.C. §143)

The above is significant as therein lays the basis for DHS to be the federal lead for cybersecurity for CI/KR and their primary role as a conduit between federal, state, local, and private sector entities. Equally important is that this wording specifically covers critical information systems and not just CI/KR, thus expanding their mandate beyond isolated CI/KR cybersecurity, but to cybersecurity of all national, state, and local critical information systems. This is later reinforced and reiterated in HSPD-7 and the NIPP; listed in the DHS responsibilities is the statement that they are responsible for "… coordinating national efforts for the security of cyber infrastructure, including precursors and indicators of an attack, and understanding those threats in terms of CIKR vulnerabilities…" (Homeland Security Presidential Directive 7, 2003; National Infrastructure Protection Plan, 2009, para. 2.2.1).

Given this codependence between provider and consumer, it would seem logical that the private sector would work closely with government agencies to harden their own CI and protect key resources. The primary issue with this logic is the fact that the private sector and government have very different motives. Private sector companies primarily exist in our capitalistic economic system with the underlying goal to maximize profits for their investors. Government agencies, such as DHS, are essentially tasked with the protection of the national instruments of power and the continuity of the quality of life standards. Security measures implemented in the private sector, beyond any formal regulation, must stand up to a rigorous consideration of return on investment as viewed through a risk management lens. Additionally, the private sector may consciously reject cybersecurity measures which, by their implementation, would subject their companies to additional compliance requirements (e.g., audits and/or external oversight). In light of

this apparently disjointed government and private-sector symbiotic relationship, Tikk (2010) identifies that the most important steps in securing national cyberspace must first be adopted at the domestic level, prior to attempting to leverage key partner nations. GAO has designated federal information security as a government-wide high-risk area since 1997, and in 2003 expanded it to include cyber CI (GAO 13–187, 2013).

3. DHS Efforts (aka: "Significant Strides")

According to the 2011 report titled Implementing 9/11 Commission Recommendations, DHS has made "… significant strides" over the last ten years in enhancing the security of the nation's critical physical and cyber infrastructure (U.S. Department of Homeland Security, 2011, p. 5).

> Current tools include the National Cybersecurity Protection System, of which the EINSTEIN cyber intrusion detection system is a key component; the National Cybersecurity and Communications Integration Center, which serves as the nation's principal hub for organizing cyber response efforts; a 2010 landmark agreement between DHS and the Department of Defense to align and enhance America's capabilities to protect against threats to critical civilian and military computer systems and networks; the National Infrastructure Protection Plan, a comprehensive risk management framework for all levels of government, private industry, nongovernmental entities and tribal partners; and implementation of the Chemical Facility Anti-Terrorism Standards to regulate security at high-risk chemical facilities. Additionally, in February 2011, President Obama announced the Wireless Innovation and Infrastructure Initiative to develop and deploy a nationwide, interoperable wireless network for public safety. None of these tools existed prior to 9/11. (U.S. Department of Homeland Security, 2011, p. 5)

The remainder of this section discusses the above significant strides by DHS to aid them in their mandate specifically for enhancing the security of critical physical and cyber infrastructure as related to the cyber domain. Therefore, this section addresses the NIPP; an agreement between DHS and the Department of Defense to align and enhance America's capabilities to protect against threats to critical civilian and military computer systems and networks; the creation of 24-hr cybersecurity common operational picture via the National Cybersecurity and Communications Integration Center (NCCIC); and the National Cybersecurity Protection System (NCPS).

a. Evolution of the National Infrastructure Protection Plan

Per the direction provided in HSPD-5 (2003), on March 1, 2004, the then newly formed DHS issued their guidance on the presidentially mandated formalization of a national emergency response framework, called the National Incident Management System. Ever since, DHS struggled to find the proper balance of interagency, state, and local interaction with the private sector. The below sub-sections provide some insight into the historic efforts of DHS to find this balance.

The end result is the National Infrastructure Protection Plan, released in 2009, as a comprehensive risk management framework for all levels of government, private industry, nongovernmental entities and tribal partners, which evolved from the significant efforts of DHS to find an acceptable means by which to protect disparate CI/KR. The below subparagraphs provide some insight into this evolution from other national plans.

(1) National Response Plan (2004). Although later amended in 2006 by DHS in response to data following an initial 240-day evaluation period, the original National Response Plan (2004) was published in December 2004 in order to provide "… a single, comprehensive framework for the management of domestic incidents" (National Response Plan, 2004, p. iii). This document is significant due to the fact that it also was accompanied by a letter of agreement (LOA) which was then signed by 32 federal departments and agencies and other organizations to commit to eight specific supporting line items in the implementation of the NRP as put forward by DHS. This was tenable primarily since the NRP did not alter the statutory responsibilities nor alter the funding of federal, state, local, or tribal departments and agencies and was built on existing systems and best practices. The important thing to note from this document though is that it tried to implement a single framework solution, regardless of the disaster being responded to. Negative feedback from dealing with various events during the evaluation period led DHS to revisit and revise their doctrine.

The NRP, officially implemented April 15, 2005, was designed to be the principal operational plan for implementing national incident management by detailing the processes and national-level coordinating structures that will be required and

used during an INS (National Response Plan, 2004, p. 16). Specifically, the NRP was stated to be an "… all-hazard, all-discipline plan…" and was the direct implementation of NIMS for events designated as *Incidents of National Significance* (INS). In a designated INS, "… the Secretary of Homeland Security, in coordination with other Federal departments and agencies, initiates actions to prevent, prepare for, respond to, and recover from the incident. These actions are taken in conjunction with State, local, tribal, nongovernmental, and private-sector entities" (National Response Plan, 2004, p. 15). The means of informing the U.S. president are established through a convening body termed the *Interagency Incident Management Group* (IIMG) (National Response Plan, 2004, p. 22). Clearly explained in the NRP, the IIMG was a "… scalable organization primarily comprised of senior-level representatives from DHS, other Federal departments and agencies, and NGOs, as required" (National Response Plan, 2004, p. 22). While stood up only at the direction of the Secretary of DHS in response to a specific INS, the IIMG replaced the Catastrophic Disaster Response Group which served as the policy-level multiagency coordination entity under the FRP (National Response Plan, 2004, p. 22).

The plan distinguishes between national-level incidents that require coordination by the DHS, which are termed INS, and the majority of incidents that were to be handled through existing emergency authorities and plans by responsible jurisdictions and agencies.

(2) National Response Framework (2008). Dated January 2008, the DHS disseminated the initial National Response Framework (NRF) as an overture to how the U.S. would respond to any natural or man-made hazard. Officially, the NRF superseded the NRP on March 22, 2008 as the plan to respond to national-level incidents. Written to capture specific authorities and best practices, the NRF is structured to be scalable, flexible, and accommodating of adaptable coordinating structures in order to best respond to the specific incident. The document outlines that the structure attempts to do this by "… aligning key roles and responsibilities across the Nation [linking all levels of government, nongovernmental organizations, and the private sector] … managing incidents that range from the serious but purely local to large-scale terrorist attacks or catastrophic natural disasters" (National Response Framework, 2008, p. 1).

Although meant to supersede the corresponding sections of the National Response Plan (2004, with 2006 revisions), this document itself was transformed from the primary plan to a subset of a larger plan three years later in 2011 with the issuance of the National Preparedness Goal directed in PPD-8. PPD-8 integrated, and required the update of, the NRF as one of five National Preparedness Frameworks of the National Planning System. The updated NRF was then released May 2013, as previously discussed in Chapter III, para. C.4.

(3) National Infrastructure Protection Plan (2009). The preponderance of U.S. CI/KR is privately owned and operated, which means ensuring its protection and resiliency involves an unprecedented partnership between government and the private sector (National Infrastructure Protection Plan, 2009). This partnership is at the heart of the National Infrastructure Protection Plan (NIPP) put forth by the DHS in 2009, which establishes a unique coordination and information-sharing framework that unifies protection of our nation's CI/KR into an integrated plan. Building from the initial CI/KR list provided in PDD-63, DHS divided the responsibilities for CI/KR protection into *Sector-Specific Agencies* (SSA) in the issuance of HSPD-7 (Homeland Security Presidential Directive 7, 2003) and further refined those responsibilities six years later in the NIPP (2009).

Critical infrastructure sector	Description	Lead agency or agencies
Agriculture and food	Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.	Department of Agriculture Department of Health and Human Services (Food and Drug Administration)
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.	Department of the Treasury
Chemical	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical sector produces products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.	DHS
Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.	DHS
Communications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.	DHS
Critical manufacturing	Transforms materials into finished goods. The sector includes the manufacture of primary metals, machinery, electrical equipment, appliances, and components, and transportation equipment.	DHS
Dams	Manages water retention structures, including levees, dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.	DHS
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	DHS
Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Government facilities	Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the U.S. and abroad.	DHS
Health care and public health	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Information technology	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.	DHS
National monuments and icons	Maintains monuments, physical structures, objects, or geographical sites that are widely recognized to represent the nation's heritage, traditions, or values, or widely recognized to represent important national cultural, religious, historical, or political significance.	Department of the Interior
Nuclear reactors, materials, and waste	Provides nuclear power. The sector includes commercial nuclear reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; the decommissioning of reactors; and the transportation, storage, and disposal of nuclear materials and waste.	DHS
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector	DHS
Transportation systems	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	DHS
Water	Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.	Environmental Protection Agency

Table 6. Critical Infrastructure Sectors and Lead Agencies
(From GAO-11-865T, 2011, Table 1)

b. Bi-lateral DHS-DoD Memorandum of Agreement (2010)

Signed in September 2010, the DHS and the DoD entered into a memorandum of agreement regarding cybersecurity, agreeing to:

> … provide personnel, equipment, and facilities in order to increase interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities. Implementing this Agreement will focus national cybersecurity efforts, increasing the overall capacity and capability of both DHS' homeland security and DoD's national security missions, while providing integral protection for privacy, civil rights, and civil liberties.

c. Cybersecurity Common Operational Picture

As an overview, Figure 2 graphically depicts the organizational chart of DHS, as retrieved from the DHS Main Page in May 2013. Accentuated in a red box is the primary directorate of concern with respect to cyber—Office of the National Protection and Programs Directorate (NPPD).

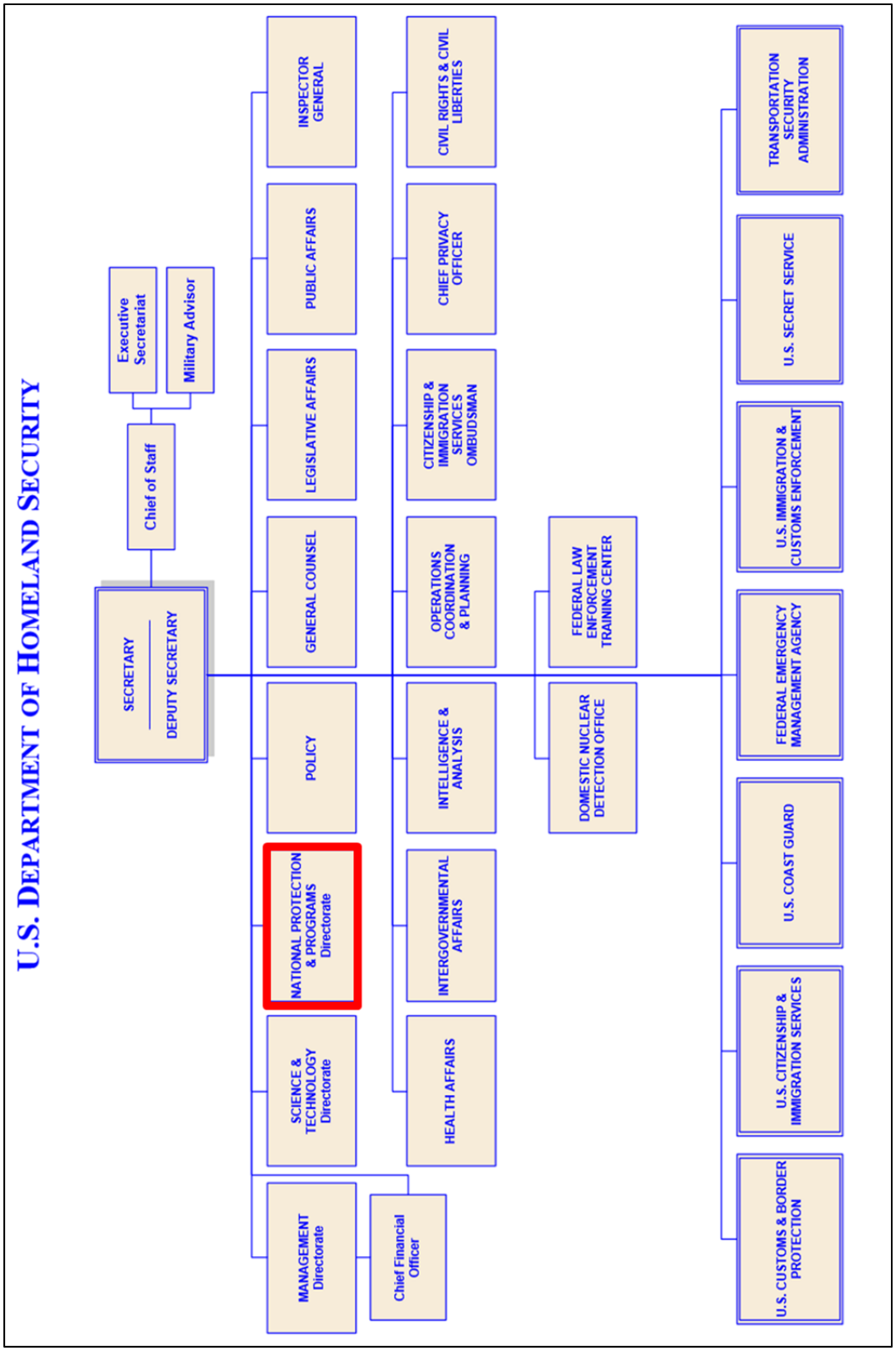

Figure 2. Organizational Chart of the Department of Homeland Security (From ICOD: April 2013)

(1) National Protection & Programs Directorate. Executive Order No. 13,618, signed July 6, 2012, disseminated the roles and responsibilities of federal agencies with respect to its title—*Assigning National Security and Emergency Preparedness Communications Functions*. In response, DHS' National Protection and Programs Directorate (NPPD) / Office of Cybersecurity and Communications (CS&C) realigned its office in October 2012 to better meet the required responsibilities set forth in the new EO (GAO-13–187, 2013, p. 95). Due to the realignment though, CS&C operational elements realigned as well to report directly to the NCCIC. This shift is significant as it bound communications and cybersecurity through the functions performed by the National Coordinating Center for Telecommunications, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and the United States Cyber Emergency Response Team (US-CERT) (GAO-13–187, 2013, p. 95).

The NPPD organizational structure, graphically depicted in Figure 3, highlights two key departments, accentuated by red box outlines. Combined they address CIP from threats originating from cyberspace—CS&C and the Office of Infrastructure Protection (IP). Although Figure 3 is from June 2011, the four bottom divisions remain valid according to the DHS NPPD web site, as of July 2013.

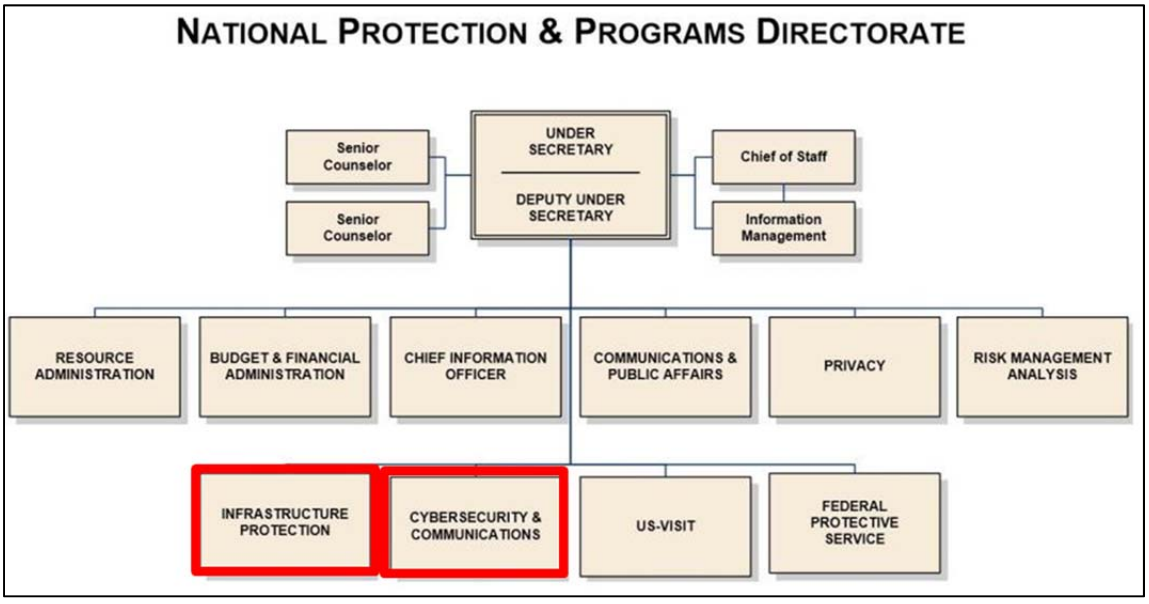

Figure 3. DHS/NPPD Organizational Chart (From ICOD, June 2011)

Fulfilling their cybersecurity roles, per the August 2012 DHS report titled *Office of Infrastructure Protection Strategic Plan: 2012–2016,* CS&C and IP collaboratively "… enhance the integration of analysis, modeling, and assessment tools and methodologies to better analyze and understand the impacts on physical infrastructure from cyber and control system exploits and develop enhanced risk management solutions" (U.S. Department of Homeland Security, 2012, p. 8).

Specifically, CS&C is tasked with assuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure. As a compliment, IP leads the coordinated national effort to reduce risk to CI/KR posed by acts of terrorism. Together, they increase the nation's level of preparedness and the ability to respond and quickly recover in the event of an attack, natural disaster, or other emergency. Part of their success can be attributed directly to the NCCIC which is aligned under CS&C.

Per the DHS report titled *Implementing 9/11 Commission Report Recommendations*, the NCCIC is a 24-hour, DHS-led coordinated watch and warning center to serving as the nation's principal hub for organizing cyber-response efforts and maintaining the national cyber and communications common operational picture (U.S. Department of Homeland Security, 2011, p. 5).

d. National Cybersecurity Protection System

To feed the NCCIC, the Network Security Deployment branch of the CS&C employs the NCPS as the DHS' program of record to provide an "… integrated system of intrusion detection, analytics, intrusion prevention, and information sharing capabilities that are used to defend the Federal Executive Branch civilian government's IT infrastructure from cyber threats" (U.S. Department of Homeland Security, 2012). The NCPS, referred to colloquially as EINSTEIN in press briefings, "… consists of the hardware, software, supporting processes, training, and services … to support the Department's mission requirements as delineated in the CNCI [Comprehensive National Cybersecurity Initiative] and mandated in NSPD-54/ HSPD-23" (U.S. Department of Homeland Security, 2012).

(1) EINSTEIN. EINSTEIN, as an evolving IDS/IPS hybrid, provides a wide range of cyber security capabilities designed to "… improve detection, prevention, and notification of cyber incidents, improve correlation, aggregation and visualization of cybersecurity data, improve information of cybersecurity activity…." on government networks (primarily the .gov domain) (U.S. Department of Homeland Security, 2012). Multiple instances of EINSTEIN are of note.

- EINSTEIN 1 was originally provided in 2008 as an intrusion detection system (IDS) and was key for detecting and logging federal civilian Executive Branch agency network traffic for analysis using standard IDS protocols of known signature based detection (U.S. Department of Homeland Security, 2013, p. 2)
- EINSTEIN 2 provided additional capabilities by alerting analysts and by providing better traffic analysis, while instituting customized signature based detection (U.S. Department of Homeland Security, 2013, p. 3)
- EINSTEIN 3 Accelerated (E^3A) is reported to be more of an intrusion protection system (IPS), which by its very nature, and in conjunction with internet service providers (ISPs), will be able to conduct very specific configuration changes to the systems monitored if rule-based criteria are met (U.S. Department of Homeland Security, 2013, p. 3)

Per the Oct 31, 2012 DHS briefing to the Data Privacy Integrity Advisory Committee, once formally instituted, E^3A will provide the following services to aid US-CERT and NCCIC:

- Intrusion detection (passive defense);
- Intrusion prevention (active defense);
- Advanced cyber analytics;
- Data aggregation & correlation;

- Visualization;
- Malware analysis;
- Packet Capture;
- Incident Management; and
- Information sharing and collaboration.

A noted limitation of the NCPS (EINSTEIN), in any version, is that it solely covers the federal civilian Executive Branch agency networks. Although useful for a common operational picture of those networks, it is not tied to state, local, or private sector systems in order to provide advance warning of probing or attacks, which may be indicative of a coordinated attack. It therefore is a useful tool for the NCCIC, but limited in value for national defense of CI/KR.

B. U.S. CODE TITLE 10

Title 10 of the U.S. Code is titled *Armed Forces* and primarily provides the statutory authorities governing the DoD as a war fighting force. As such, the remainder of this section will look at DoD authorities, roles and efforts as they relate to cybersecurity and the protection of CI/KR.

According to the *National Military Strategy for Cyberspace Operations (2006)*, the U.S. can achieve superiority in cyberspace only if command and control relationships are clearly defined and executed. DoD has assigned authorities and responsibilities for implementing cyberspace operations among combatant commands, military services, and defense agencies; however, the "… supporting relationships necessary to achieve command and control of cyberspace operations remain unclear" (GAO Report 11–75, 2011). What is clear though is that cyberspace operations are increasingly essential to defeating the sensors and C2 that underpin an opponent's capabilities (Greenert, 2011). As such, USSTRATCOM, via the Unified Command Plan, is assigned specific responsibilities which include planning, synchronizing, advocating, and employing capabilities to meet the United States' strategic deterrence and cyberspace operations (Feickert, 2013, p. 20).

1. DoD Authorities

The DoD has both constitutional authority, as delegated by the U.S. president, and statutory authorities, as approved by the U.S. Congress. Title 10 created and empowered the Secretary of Defense (SECDEF) with all the “authority, direction and control” over DoD, including subordinate agencies and commands (10 U.S.C. §113, sect. (b)).

In a personal interview with the DoD Senior Associate Deputy General Counsel for Intelligence, Walter Gary Sharp, Sr., on January 15, 2013, Sharp identified four primary DoD missions that had adequate authorities relating to cyberspace: (1) homeland defense; (2) protecting and defending DoD information systems (including the DIB); (3) protecting and defending non-DoD information systems; and (4) emergency support. These four mission areas are detailed below, citing the requisite constitutional and/or statutory authorities. For the sake of consolidation, however, the protection and defense of information system roles have been subordinated under the following section on homeland defense.

a. Homeland Defense

In 1941, while still in a neutral position before being drawn into WWII, U.S. Attorney General Robert Jackson provided the following analysis with respect to the U.S. president's military powers:

> Article II, section 2, of the Constitution provides that the President "shall be Commander in Chief of the Army and Navy of the United States." By virtue of this constitutional office he has supreme command over the land and naval forces of the country and may order them to perform such military duties as, in his opinion, are necessary or appropriate for the defense of the United States. These powers exist in time of peace as well as in time of war. (Yoo, 2001, sect. II)

As such, U.S. Constitution (Article II, sect. 2), authorizes the U.S. president to direct the defense of the Nation as a primary duty. This interpretation was later reaffirmed by U.S. Congress in both the “… War Powers Resolution, Pub. L. No. 93-148, 87 Stat. 555 (1973), codified at 50 U.S.C. §1541-1548, and in the Joint Resolution passed by Congress on September 14, 2001, Pub. L. No. 107-40, 115 Stat. 224 (2001)” (Yoo, 2001). Due to the scope of the task, this constitutional authority is

delegated via statutory authority to the SECDEF and, subsequently upon presidential direction, commanders of combatant commands as the lead, and supported, department for national defense (3 U.S.C. §301-303; 10 U.S.C. §113; 50 U.S.C. §401, sect. 2; 10 U.S.C. §164).

Under the responsibilities granted through these authorities: appropriately measured DoD response to hostile acts or hostile intent, through conventional or non-conventional means (e.g., offensive cyberspace operations) retain "… clear Constitutional authority"; defensive response actions, which are still being developed, (e.g., countermeasures) remain "… untested Constitutional authority" (Sharp, 2012, slide 12).

Defense of the nation, with respect to cybersecurity, can be further broken down into protecting and defending both DoD and non-DoD information systems.

(1) Protect and Defend DoD Information Systems. While retaining the same above authorities from the homeland defense section, with respect to the GIG, the DoD is provided with: "… robust statutory authority" to conduct network operations (Sharp, 2012, slide 12).

(2) Protect and Defend Non-DoD Information Systems. While the ability to share or provide technical expertise and information is still evolving, the DoD retains "… adequate statutory authority" to do so (Sharp, 2012, slide 12).

b. Emergency Authorities

Involvement in a designated national emergency resulting from an INS, as solicited by the DHS, does not have clear constitutional basis but does retain some aging statutory authority (Sharp, 2012, slide 12).

While three additional key pieces of legislation leverage DoD assets in execution of national objectives — Posse Comitatus Act, Stafford Act, and Economy Act — only two have validity with respect to the cyber domain and those capabilities residing within DoD to aid in post-INS events. The Posse Comitatus Act does not apply to this situation in a post-INS cyber-related scenario. Therefore, the remainder of this section will briefly describe the authorities provided by the other two acts, and conclude with how they relate to cyber protection of CI/KR.

(1) Stafford Act. Augmenting the previous discussion in Chapter II, para. C.2.d, the Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988 amended the Disaster Relief Act of 1974 (Public Law No. 93–288). This provides the legal means by which the DoD can support disaster response activities. As there are no limitations on the disaster once designated as an INS, it must be assumed that this is also inclusive of those involving the cyber domain. This in no way precludes the applicable statutory authorities that DoD must operate under.

(2) Economy Act. The Economy Act of 1932 (Pub. Law No. 72–212; 47 Stat. 382), as amended, provides for the reimbursement for goods and services of support from one federal agency when requested by a separate federal agency. As the requesting agency may not have the federally mandated mission to maintain a specific capability or skillset as a means to fulfill their mission, but does knows that the requested agency does, the Economy Act of 1932 allows for the utilization of the capability on a not to interfere basis with the knowledge that the requesting agency is required to monetarily reimburse affected agency. This law minimizes unnecessary duplication of capabilities and thus attempts to act a good steward of tax payers' dollars.

This law is applicable to cybersecurity in that DoD, through USCYBERCOM and the National Security Agency (NSA), maintain unique cyber capabilities and access which may be required by either DHS or DOJ in a post-incident response involving the cyber domain.

2. DoD Existing Role

It is important to note when reviewing the mission and capabilities, that according to the OMB FY2013 report of the federal budget for the homeland security mission, the DoD receives approximately 26% of total federal homeland security funding, second only to that of the DHS itself (OMB, 2013). To have such a significant portion of the budget for domestic defense, it would stand to reason that DoD must also have a significant mission to perform in justification. The fact is that it does.

> The Department of Defense (DoD) protects the U.S. homeland through two distinct but interrelated missions: (1) *homeland defense*, which defends against threats such as terrorism, weapons of mass destruction,

> and cyber incidents; and (2) *civil support*, which involves supporting other federal agencies in responding to major domestic disasters, emergencies, and special events. (GAO Report 13–128, 2012)

On October 1, 2002, DoD announced the operational capability of the newly established U.S. Northern Command (USNORTHCOM), which was created to consolidate existing homeland defense and civil support missions that were previously executed by other military organizations. Despite this, some of the homeland defense mission set falls clearly on U.S. Strategic Command (USSTRATCOM), even more so now that USSTRATCOM has the sub-unified command U.S. Cyber Command (USCYBERCOM).

a. Homeland Defense

Fully comprehending the enormity of the task assigned and the decentralized execution of the cyber vulnerability existing in networks paired with the cyber threats that are posed by nation-states and non-nation state actors alike, emphasis and visibility on cyber operations increased to the point that a new sub-unified command under USSTRATCOM was established on May 21, 2010—USCYBERCOM (Feickert, 2013, p. 20).

In preparation, SECDEF guidance dated June 23, 2009, detailed that, as delegated by USSTRATCOM, USCYBERCOM would be responsible for executing the specified cyberspace missions detailed in Section lS.d.(3) of the Unified Command Plan (UCP). These missions are essentially "… to secure our freedom of action in cyberspace and mitigate the risks to our national security that come from our dependence on cyberspace and the associated threats and vulnerabilities" (Alexander, 2009).

Being the lead in the proactive defensive role, DoD implemented measures to better address cybersecurity threats to the nation, such as developing new organizational structures, first led by the establishment of the USCYBERCOM and service specific cyber commands/elements, to facilitate the integration of *cyberspace operations* with a focus on *cybersecurity* (GAO Report 11–75, 2011). This is important as DoD maintained the responsibility to both defend the GIG and the national DIB.

(1) Protection of the Global Information Grid. With the goal of protecting the GIG in mind, U.S. Cyber Command recognized that they must incorporate integrated defensive and offensive cyberspace operations into all planning efforts to span the relevant dimensions of cybersecurity (GAO Brief 11–695R, 2011). This gets problematic, as Jensen (2010) states that 98% of all U.S. government communications travel over civilian-owned-and-operated networks, making much of this intermixed infrastructure legitimate targets under the *Law of Armed Conflict* (LOAC) and therefore in need of protection. The current integration of U.S. government assets with civilian systems makes segregation impossible and therefore creates a legal responsibility for the U.S to protect those civilian networks, services, and communications under LOAC (Jensen, 2010). According to Breen and Geltzer (2011), the decentralized structure of the Internet itself intensifies the overall threat, as it encourages state and non-state actors alike to develop and employ cyber warfare capabilities anonymously, making deterrence more complicated.

(2) Protection of the Defense Industrial Base. Per the CI/KR sector assignment to SSAs in the NIPP (2009), DoD developed an annex detailing their plan to execute those duties and responsibilities and updated it in 2010 (NIPP Annex—DIB Security Specific Plan, 2010).

Although protection can include a wide range of activities from improving security protocols, hardening facilities, building resiliency and redundancy, initiating active or passive countermeasures, installing security systems, and leveraging "… self-healing" technologies, it also includes implementing cybersecurity measures (NIPP, 2009). In an effort to define the threats which the measures must be paired to, Tikk (2010) has broken cybersecurity down to four relevant dimensions—Internet Governance, Cyber Crime, Cyber Terrorism, and Cyber Warfare. So, while even though the actual characterization of cyberspace activity remains the subject of much debate in the academic and technical realm, the unique nature of the cyber arena clearly calls into question traditional state boundaries and operational codes of conduct (Dobitz, Hass, Holtje, Jokerst, Ochsner, & Silva, 2008).

The task of securing the cyber domain must truly be both a national and international one; DoD is uniquely poised to foster greater information sharing, with respect to cybersecurity, amongst partner nations (Tikk, 2010). Despite somewhat differing national views on cybersecurity priorities, cooperation has proved successful among like-minded partners, and there are signs of emerging cyber-coalitions although greater coordination will be required to address future threats (Tikk, 2010). The DoD, DHS, private sector CI/KR owners/operators and others are improving: (1) physical, personal, and cyber security; (2) risk-based investment decision-making; and (3) information sharing throughout the DIB sector, forging a foundation by which to unify individual goals toward a more transparent cooperative effort (NIPP Annex–DIB Security Specific Plan, 2010). In line with holistic view of Tikk (2010), DoD has implemented strict information assurance (IA) requirements for their information technology systems, not only on federal systems, but strict implementation of standards across coalition networks and in the defense industry (NIPP Annex–DoD's Security Specific Plan, 2010).

b. Civil Support

The civil support role of the DoD was solidified by Executive Order No, 12,148 (1979) nearly 35 years ago. In this EO, it states that "… the Secretary of Defense shall provide the Director of the Federal Emergency Management Agency with support for civil defense programs in the areas of program development and administration, technical support, research, communications, transportation, intelligence, and emergency operations" (Executive Order No. 12, 148, 1979, para. 2–205). Additionally, HSPD-8 (2003) explicitly stated that the DoD will provide the DHS with information describing the organizations and functions within the DoD that may be utilized to provide support to civil authorities during a domestic crisis (Homeland Security Presidential Directive 8, 2003, para. 21). More recently, this concern was addressed in the memorandum of agreement between the DHS and the DoD in 2010 and previously described in this chapter, para. A.3.b. Despite these efforts, critics and skeptics remain.

> While a 2010 DoD Directive, a 2007 joint publication, and an agreement with the Department of Homeland Security (DHS) provide some details on

> how DoD should respond to requests for civil support in the event of a domestic cyber incident, they do not address some aspects of how DoD will provide support during a response. First, DoD has not clarified its roles and responsibilities, and chartering directives for DoD's Offices of the Assistant Secretaries for Global Strategic Affairs and for Homeland Defense and Americas' Security Affairs outline conflicting and overlapping roles and responsibilities. Second, DoD has not ensured that its civil support guidance is aligned with national plans and preparations for domestic cyber incidents. (GAO Report 13–128, 2012).

3. DoD Efforts

"DoD has issued and updated several key pieces of doctrine, policy, and strategy for homeland defense and civil support, but it has not updated its primary Strategy for Homeland Defense and Civil Support since it was initially issued in 2005" (GAO Report 13–128, 2012). DoD has, however: (1) published an internally deconflicted standardized lexicon with respect to cyber; (2) published DoD guidance for the internally standardized handling of cyber-incident procedures; and (3) been working through the Office of the Under Secretary of Defense–Policy (OUSD-P) to address an interagency approach to national cybersecurity.

a. Standardized Cyber-Lexicon

The DoD Joint Publication 3–12 (*Cyberspace Operations*), signed on February 5, 2013, provides the deconflicted acceptable cyber-lexicon for DoD. This standardization effort paves the way for future efforts of interagency deconfliction and standardization.

b. Standardized DoD Cyber-Incident Response Procedures

The Chairman of the Joint Chief of Staff Manual 6510.01B, titled *Cyber Incident Handling Program* and published on July 10, 2012, details the deconflicted cyber incident handling program for DoD. This standardization effort focuses on the DoD responsibility to protect DoD information systems and the DIB, as their assigned CI sector in the NIPP through the creation and utilization of a Joint Incident Management System (Joint Chief of Staff Manual 6510.01B, 2012, encl. F(appx. B)).

c. Interagency Cooperation

From a specific recommendation, originating from the same 2012 GAO report, that the Secretary of Defense should direct the Under Secretary of Defense for Policy to work with USSTRATCOM and its subordinate sub unified command (USCYBERCOM), DHS, and other relevant stakeholders to update guidance on preparing for and responding to domestic cyber incidents to align with national-level guidance, Figure 4 has been generated (GAO Report 13–128, 2012). Colloquially referred to as the *Bubble Chart*, Figure 4 lists and graphically depicts the agreed upon responsibilities, shared and individual, of the three primary federal departments responsible for national cybersecurity.

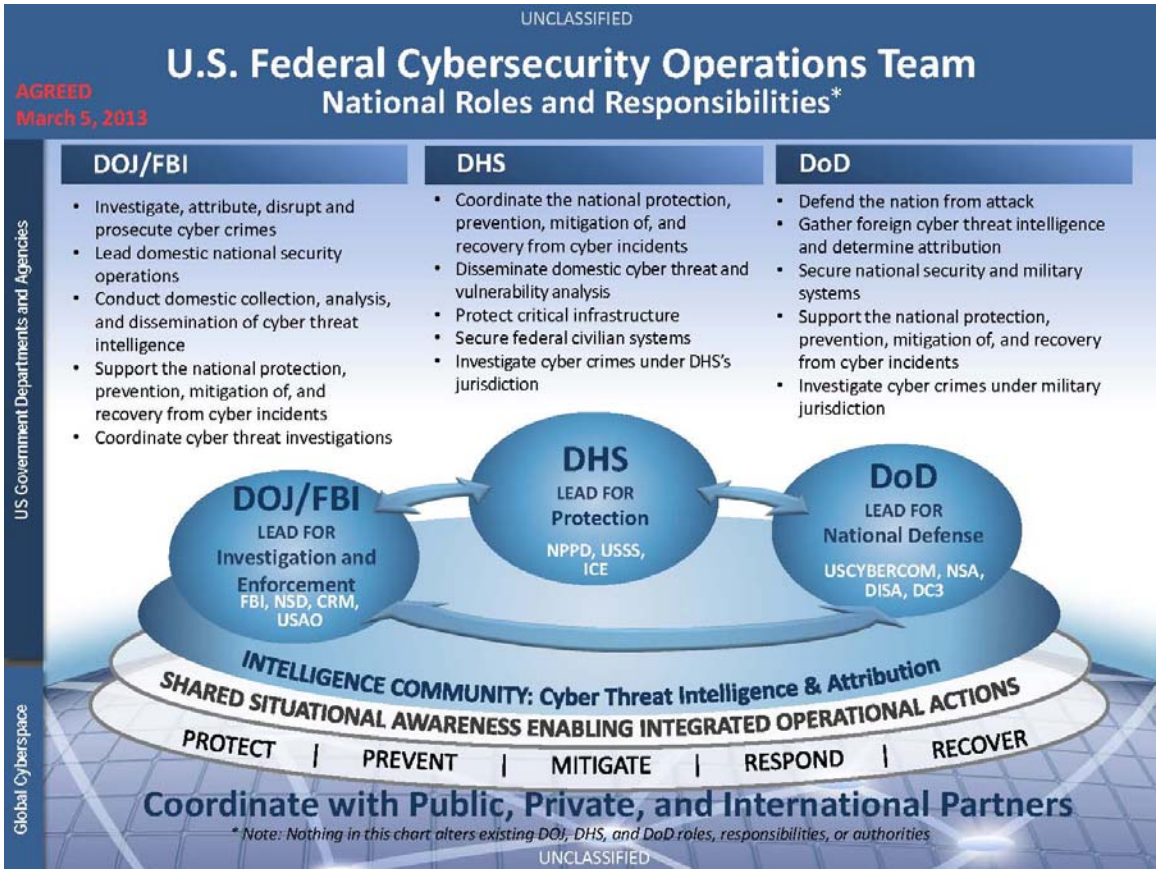

Figure 4. U.S. Federal Cybersecurity National Roles and Responsibilities (From ICOD, May 2013)

C. U.S. CODE TITLE 18

Title 18 of the U.S. Code is titled *Crimes and Criminal Procedure* and primarily provides the statutory authorities governing the DOJ. As such, the remainder of this section will look at DOJ authorities, roles and efforts as they relate to cybersecurity and the protection of CI/KR.

With regard to criminal activities, the cyber domain is simply an environment within which an otherwise already illegal act is executed. So, while not all laws are clearly cyber-related, many crimes may be perpetrated utilizing the cyber domain and thus require expertise internal or external to properly investigate and document for prosecutorial purposes. As the Department of Justice (DOJ) is the lead executive department for these federal law enforcement responsibilities, it therefore works collaboratively with other executive agencies as the supported executive department of the U.S. government in those duties. Be that as it may, the nature of their involvement is therefore after an identified crime has occurred and does in no way include prevention, although sharing of information may mitigate additional criminal actions.

Specifically, in violation of U.S. federal laws such as the unauthorized and unlawful access, exploitation, or modification of CI/KR-related information and control systems, the DOJ is key in evidentiary gathering/control, arrest and prosecution.

1. DOJ Authorities

Utilizing their constitutional authority, the U.S. Congress, per the Act to Establish the Department of Justice (Pub. Law No. 41-97, 16 Stat. 162 (1870)), established the DOJ to exercise control over: (1) all criminal prosecutions; (2) civil suits in which the United States maintains an interest; and (3) federal law enforcement. Ultimately vested in the U.S. Attorney General via statutory authority (28 U.S.C. §503), the propensity of duties have been further delegated internal to the various DOJ departments, as provided for via statutory authority (28 U.S.C. §510).

Key among the statutory authorities is the authority to enforce federal law. As such, it assists to provide the scope in which those laws pertaining to cybersecurity are

framed. The fundamental cybersecurity related law, which pertains to CI/KR, is the Computer and Fraud Abuse Act of 1986.

a. Computer Fraud and Abuse Act of 1986

Due to its fundamental significance to the issue of the legality of cyber-attacks and intrusions into U.S. information systems, the below is the exact excerpt from the Computer Fraud and Abuse Act, as amended and implemented in 18 U.S.C. §1030. Having undergone multiple amendments by way of maturation of cybersecurity knowledge and practice, the law in its current form covers seven distinct categories of illegal access and use of U.S. computer systems. The law states:

> (a) Whoever—
>
> (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> > (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
> >
> > (B) information from any department or agency of the United States; or
> >
> > (C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

> (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;
>
> shall be punished as provided in subsection (c) of this section. (18 U.S.C. §1030)

Although not the entirety of 18 U.S.C. §1030, the above nonetheless provides some insight into the level of detail with which law enforcement and investigative officers must delve to arrest and prosecute individuals suspected of breaking into national CI/KR systems. Boiled down to bite-size generalizations, the seven sections are:

(1) Computer espionage;

(2) Computer trespassing to obtain government or financial information;

(3) Computer trespassing in a government computer;

(4) Committing fraud with a protected computer;

(5) Damaging a protected computer (e.g., viruses, worms);

(6) Trafficking in passwords of a government or commerce computer; and

(7) Threatening to damage a protected computer.

Overlooking the broad generalizations, of the above categories, the less obvious offense is listed in 18 U.S.C. §1030(a)(4); intentionally included in the above is the topic of fraud. Unauthorized access often is obtained by fraudulent means (e.g., fake password reset, fraudulent solicitation) and thus constitutes an illegal act even if actual access to the information system utilized a valid username and password which had been supplied the authorized access. The July 2013 McAfee report titled *The Economic Impact of Cybercrime and Cyber Espionage* reinforces this concept by stating that cybercrime is "… usually based on impersonating individuals to gain access to their financial resources or other forms of fraud, such as impersonating an antivirus company in order to persuade individuals to pay to have their computers cleaned" (McAfee, 2013, p. 10).

2. DOJ Existing Roles

The DOJ has been granted the ability to issue warrants, make arrests, and conduct various law enforcement activities necessary to document justification for either. Toward the investigative aspect, while statutory authority authorizes some specific collection methods, it stands to reason that the DOJ is not uniquely positioned to have access to all of the cyber information or databases needed. Therefore, information sharing between the DOJ and other executive departments (e.g., DHS and DoD) becomes necessary.

In October of 1998, PDD-63 created the National Infrastructure Protection Center at the Federal Bureau of Investigations (FBI) with the intent to integrate DoD, FBI, Secret Service, Department of Energy, Department of Transportation, intelligence community (IC), and private sector representatives to increase information sharing among agencies and the private sector. The National Infrastructure Protection Center also provided the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts.

While not completely abandoned, interagency coordination in support of a legal solution is now directed by HSPD-7 (2003), which directs support of the "… Department of Justice and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law" (Homeland Security Presidential Directive 7, 2003, para. 16).

As such, some of the critical statutory authorities for DOJ, which enable these exchanges and compliment the other executive agencies, are those governing information intercept, information sharing, and arrests.

a. Information Intercept

There reside two primary categories within information intercept—routine and emergency.

(1) Routine. Statutory authority authorizes the routine intercept role of the DOJ for wire taps, and states that DOJ "… may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant …

an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation…" (18 U.S.C. §2516).

Additionally, statutory authority authorizes the routine intercept role of the DOJ for use of a pen register or trap and trace, as it authorizes "… the installation and use of a pen register or trap and trace device anywhere within the United States, if … the information likely to be obtained … is relevant to an ongoing criminal investigation" (18 U.S.C. §3123).

(2) Emergency. Statutory authority authorizes the emergency intercept role of the DOJ for wire taps. Specifically, Title 18 states that any investigative or law enforcement officer who reasonably determines that:

> (a) an emergency situation exists that involves—
>
> (i) immediate danger of death or serious physical injury to any person,
>
> (ii) conspiratorial activities threatening the national security interest, or
>
> (iii) conspiratorial activities characteristic of organized crime, that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and
>
> (b) there are grounds upon which an order could be entered under this chapter to authorize such interception. (18 U.S.C. §2518, para. 7)

Additionally, statutory authority also authorizes the emergency intercept role of the DOJ in the use of a pen register or trap and trace. Specifically, Title 18 also authorizes any investigative or law enforcement officer, who reasonably determines that:

> (1) an emergency situation exists that involves—
>
> (A) immediate danger of death or serious bodily injury to any person;
>
> (B) conspiratorial activities characteristic of organized crime;

(C) an immediate threat to a national security interest; or

(D) an ongoing attack on a protected computer … that constitutes a crime punishable by a term of imprisonment greater than one year;

that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use. (18 U.S.C. §3125, para. (a))

b. Information Sharing

In the first year under the new administration of President George W. Bush, the USA Patriot Act of 2001 was passed to broaden statutory authorities in response to the horrific acts perpetrated on September 11, 2001 (9/11). This legislation, reauthorized in 2005, provided a range of controversial tools to support law enforcement capabilities to combat terrorism, including enhancing law enforcement's electronic surveillance capabilities (Cyber Policy Review, 2009).

(1) DOJ to Government (Voluntary). The most significant tool added in the scope of this document, as it relates to cybersecurity of CI/KR, is the amendment of 18 U.S.C. §2517 which allows for information sharing from the DOJ with other governmental entities. This statutory authority specifically states that:

> Any investigative or law enforcement officer, or other Federal official in carrying out official duties …, who …, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. (18 U.S.C. §2517, para. 8)

(2) Private Sector to Government (Voluntary). Another tool, as it relates to cybersecurity of CI/KR, is found in 18 U.S.C. §2702, which allows for information sharing from the private sector with governmental entities. This statutory

authority specifically states that a provider of remote computing service or electronic communication service to the public may divulge the contents or a record of other information pertaining to a subscriber to or customer of such service "… to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency…" (18 U.S.C. §2702, para. (b)(8) & (c)(8)).

c. Arrests

Another key aspect to cybersecurity of CI/KR is the legal resolution (colloquially referred to as the legal finish), normally occurring post-event, which can only be legally executed by law enforcement and investigative professionals. Pursuant to statutory authority granted in 18 U.S.C. §3052, the FBI may "… make arrests without warrant for any offense against the United States committed in their presence, or for any felony cognizable under the laws of the United States if they have reasonable grounds to believe that the person to be arrested has committed or is committing such felony" (18 U.S.C. §3052).

Many felonies exist that require special attention, but below are a few of the key ones related to CI/KR—economic espionage, theft of trade secrets, and intellectual property rights. These three remain a key federal concern to CI/KR protection, as private sector companies maintain proprietary information, systems and protocols in their informational command and control. Competitors, or hostile actors, with inside knowledge or access gain more than simply an unfair advantage as they may gain dangerous access to how the systems are designed to enforce the confidentiality, integrity, and availability aspects of those U.S. systems. While the security of the system should not be dependent on the design or code being secret, nevertheless, an adversary is at a disadvantage if they do not have access to it.

(1) Economic Espionage (18 U.S.C. §1831). Per the Economic Espionage Act of 1996, "Economic Espionage is (1) whoever knowingly performs

targeting or acquisition of trade secrets to (2) knowingly benefit any foreign government, foreign instrumentality, or foreign agent" (18 U.S.C. §1831).

(2) Theft of Trade Secrets (18 U.S.C. §1832). Much along the same lines as economic espionage, the theft of a trade secret with the intent to undermine the owner of the trade secret, or profit someone other than the owner of the trade secret, may compromise CI/KR as many of the components and protocols used are proprietary.

(3) Intellectual Property Rights (15 U.S.C. §8101 et seq.). Intellectual property rights crimes are covered under Pub. Law No. 109-9, Title I, Sec. 105; 119 Stat. 222, which was enacted on April 27, 2005.

3. DOJ Efforts

DOJ is as active as DHS and DoD on the issue of cybersecurity, but given the nature and breadth of their mandate, their notable efforts will be minimized to two for the sake of brevity. Those two significant achievements are the update and dissemination of DOJ near-term and strategic goals and the creation of a network of like-minded attorneys and experts to specifically address cybercrime.

a. Updated DOJ Strategic Goals

As of February 2012, U.S. Attorney General Eric H. Holder, Jr. outlined, in the foreword of a document titled *DOJ Strategic Plan for Fiscal Years 2012–2016,* the DOJ priorities over the next 5 years to include the following three strategic goals:

> Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law;
>
> Goal 2: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law; and
>
> Goal 3: Ensure and Support the Fair, Impartial, Efficient, and Transparent Administration of Justice at the Federal, State, Local, Tribal, and International Level. (U.S. Department of Justice, 2012, Foreword)

The first two of the above DOJ goals are directly applicable to cybersecurity and the protection of CI/KR as crime and terrorism are the largest concerns.

As such, this leads me to the second major DOJ effort, as in response to invasions into, and cyber-attacks against, U.S. CI/KR information systems, the DOJ launched a nationwide network to better address cyber intrusions and attacks—National Security Cyber Specialist (NSCS) network.

b. National Security Cyber Specialist Network

The NSCS network, formally created in June 2012, is comprised of nearly 100 prosecutors from U.S. Attorney's offices nationwide and cyber experts from DOJ's National Security Division and Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) (U.S. Department of Justice, 2012). This network is a critical part of the department's efforts to better address cyber intrusions by focusing on the utilization of a whole-of-government approach to combating cyber threats to national security. In addition, the network is "… forging a variety of private and public sector alliances to help prevent such attacks and intrusions" (U.S. Department of Justice, 2012).

Although numerous legislation exists which govern and guide these efforts, the most pertinent and notable piece of cybersecurity legislation is the Computer Fraud and Abuse Act of 1986, as amended and previously described.

D. U.S. CODE TITLE 32

Title 32 of the U.S. Code is titled *National Guard* and primarily provides the statutory authorities governing both the Army National Guard and Air National Guard.

The Army National Guard and Air National Guard units, governed by Title 32 statutory authority, are important state and federal resources available for planning, preparing, and responding to natural or manmade incidents. This is important as, collectively, the National Guard, created via constitutional authorities, have expertise in critical areas, some being cybersecurity, recovery and information systems (U.S. Constitution, Art. I, sect. 8, cl. 16). Their involvement in federal, state, and local exercises aid to bridge a gap in socialization of the importance of, and additional resources for, emergency response to CI/KR disasters.

It is important to recall that INS will be determined after the occurrence and that support for state, local and private entities is only provided: (1) when requested; and (2) when required recovery and mitigation efforts exceed the resources and/or capabilities of the affected entity. Therefore, through greater exposure, inclusion and exposure of the numerous National Guard units, timely requests for assistance are more likely as the respective governor may activate elements of the National Guard to support state domestic civil support functions and activities. Additionally, "… the state adjutant general may assign members of the Guard to assist with state, regional, and Federal civil support plans…." if deemed necessary (National Response Framework, 2013, p. 14).

E. U.S. CODE TITLE 40

Title 40 of the U.S. Code is titled *Public Buildings, Properties and Works* and primarily provides two key statutory authorities of note with respect to CI/KR: (1) the governance of information technology procurement; and (2) law enforcement.

1. Information Technology Procurement

Simply put, 40 U.S.C. §11314, describes the statutory authorities that exist by which the head of each executive agency is permitted to acquire information technology independently. As each executive agency head is required to maintain their respective agency material readiness, this is especially applicable to the CI/KR discussion as the significant disparity of systems creates stovepipes and inadvertent barriers in interagency cooperation.

2. Law Enforcement

On a divergent topic, Title 40 specifically provides statutory authority for the DHS to designate employees to exercise a law enforcement role, in the role of physical protection of federal property, personnel on the property, and personnel exercising lawful duties in the proximity of the property (40 U.S.C. §1315). This will appear off topic, until it is considered that cybersecurity threats also include both an insider access threat vector as well as that of industrial and/or national espionage. In either case, discovery would

mandate the lawful response of a trained physical security force and, through Title 40, this makes it legal.

F. U.S. CODE TITLE 42

Title 42 of the U.S. Code is titled *Public Health and Welfare* and primarily provides the national policy with respect to the protection of CI/KR, as enacted by the Critical Infrastructures Protection Act of 2001 as quoted at the beginning of this chapter. (42 U.S.C. 5195c, sect. c(1)).

G. U.S. CODE TITLE 44

Title 44 of the U.S. Code is titled *Public Printing and Documents* and primarily provides the statutory authorities governing information resources management of all the executive agencies, specifically including federal information policies.

Protecting federal government information systems is the topic of 44 U.S.C., Chapter 35. As alluded to in the preceding section, the head of each executive agency is required to execute their respective "… agency's information resources management activities to improve agency productivity, efficiency, and effectiveness" (44 U.S.C. §3506). This statutory authority also requires the head of each executive agency to designate a Chief Information Officer, whom is responsible, with respect to federal information technology, to:

> (1) implement and enforce applicable Government-wide and agency information technology management policies, principles, standards, and guidelines:
>
> (2) assume responsibility and accountability for information technology investments;
>
> (3) promote the use of information technology by the agency to improve the productivity, efficiency, and effectiveness of agency programs, including the reduction of information collection burdens on the public and improved dissemination of public information;
>
> (4) propose changes in legislation, regulations, and agency procedures to improve information technology practices, including changes that improve the ability of the agency to use technology to reduce burden; and

> (5) assume responsibility for maximizing the value and assessing and managing the risks of major information systems initiatives. (44 U.S.C. §3506)

This responsibility inherently includes the adherence to cybersecurity standards to maximize information security, federal policy adherence and departmental policy generation.

Although many of the executive agencies do not have direct control over their allocated CI/KR sectors, as designated in the NIPP, DoD utilizes some of their statutory authorities granted by both Title 40 (e.g., contract management) and Title 44 (e.g., CIO prescription of information systems requirements) in requiring the DIB's compliance to several key cybersecurity best practices.

It should be noted that the U.S. Congress proposed a bill as recent as 2010 titled *Protecting Cyberspace as a National Asset Act of 2010* (Senate Report No. 111-368), which would have increased the information sharing between executive agency information systems for the purpose of increasing joint situational awareness. The bill never passed and Title 44 was not amended.

H. U.S. CODE TITLE 50

Title 50 of the U.S. Code is titled *War and National Defense* but essentially covers intelligence collection, intelligence activities, and covert action (Wall, 2012, p. 87). As such, Title 50 primarily provides the statutory authorities governing the formation of the National Security Council and their respective duties to advise the U.S. president with respect to the integrated and efficient activities of the U.S. government in national defense (50 U.S.C. §402, sect. a). As the title suggests, the National Security Council is the overall national coordinating body responsible for the integration between the disparate federal agencies to:

> (1) to assess and appraise the objectives, commitments, and risks of the United States in relation to our actual and potential military power, in the interest of national security, for the purpose of making recommendations to the President in connection therewith; and

> (2) to consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security, and to make recommendations to the President in connection therewith. (50 U.S.C. §402, sect. b)

Specific to the focus of Title 50, and to assist in this endeavor, it also creates the national position of the Director of National Intelligence (DNI) to prioritize, coordinate and deconflict national intelligence collection and dissemination efforts of the IC (50 U.S.C. §403-1). Although the IC is broad in their various mandates, not all of the twelve categories listed by the National Security Act of 1947, as codified in 50 U.S.C. §401(a), have a direct mission with respect to national cybersecurity and protection of CI/KR. Therefore, the remainder of this section will look at these authorities, roles and efforts as they relate to cybersecurity and the protection of CI/KR. As such, this discussion will focus on the National Security Agency (NSA) and Central Intelligence Agency (CIA).

1. National Security Agency

> The National Security Agency (NSA) performs electronic surveillance to collect foreign intelligence information for the military and policymakers. […] NSA's electronic surveillance activities are subject to strict regulation by statute and Executive Order due to the potential intrusiveness and the implications for the privacy of U.S. persons of these activities. NSA's electronic surveillance activities are also subject to oversight from multiple bodies within all three branches of the government. These safeguards have ensured that NSA is operating within its legal authority. (Congressional Record, 2000)

a. NSA Authorities

Definitively citing the exact congressional statutory authorities of the NSA, beyond personnel and training management, is relatively difficult. Pursuant to Title 50 (Chapter 47), as authorized by the National Security Agency Act of 1959 (Public Law 86–36; 73 Stat. 63; approved May 29, 1959) and amended through Public Law 112–87 (Enacted January 3, 2012), U.S.C. provides that "…nothing in this chapter or any other law … shall be construed to require the disclosure of the organization or any function of the National Security Agency…" (50 U.S.C. §3605). Better fidelity of the NSA responsibilities is possible though through Executive Order No. 12,333 and the declassified version of NSD-42. The next section, which addresses roles, will provide

better insight into those. What is clear from the U.S.C. is that NSA has been given primacy for signals intelligence (SIGINT) and is responsible to both the Secretary of Defense and the Director of National Intelligence (50 U.S.C. §403-5, sect. a(1)). Additional statutory authorities granted for execution of their support to cybersecurity as it relates to national CI/KR include both law enforcement role and law enforcement support roles.

(1) Law Enforcement. Odd to not foresee, but Title 50 also grants NSA employees with some limited law enforcement authorities in line with those granted to DHS employees in Title 40. As such, NSA employees may be designated to exercise a physical security force by using these authorities:

> (A) at the National Security Agency Headquarters complex and at any facilities and protected property which are solely under the administration and control of, or are used exclusively by, the National Security Agency; and
>
> (B) in the streets, sidewalks, and the open areas within the zone beginning at the outside boundary of such facilities or protected property and extending outward 500 feet. (50 U.S.C. §3609, sect. a)

Modeled after those authorities granted in Title 40 to the DHS personnel, this statutory authority provides a physical defense-in-depth. These statutory authorities are essential as the NSA retains the offensive cyber capabilities, which can be used to disrupt ongoing attacks on the national CI/KR or as a deterrent for additional cyber-attacks or incursions.

(2) Law Enforcement Support. Title 50 also grants statutory authority for the NSA to, "… upon the request of a United States law enforcement agency, collect information outside the United States about individuals who are not United States persons … to use the information collected for purposes of a law enforcement investigation or counterintelligence investigation" (50 U.S.C. §403-5a, sect. a).

b. NSA Role

Although not statutory authority, Executive Order No. 13,470 (signed July 30, 2008), titled *Further Amendments to Executive Order 12333, United States*

Intelligence Activities, amends Executive Order No. 12,333 (December 4, 1981) and sheds some light on the expectation levied on NSA by updating intelligence collection roles of national intelligence agencies. The amended EO states that the NSA shall:

> 1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;
>
> (2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director [DNI];
>
> (3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;
>
> (4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;
>
> (5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;
>
> (6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director [DNI];
>
> (7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and
>
> (8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this

> order. (Executive Order No. 12,333, as amended 2008, para. 1.7(c))

This EO, even through multiple amendments, reaffirms with significant evidence that NSA is the primary agency in charge of SIGINT. What is not clear is the extent that SIGINT differs from cyber intelligence, as the root document (NSD-42) essentially predates extensive maturation of the cyber domain.

Declassified in 1996, NSD-42 (signed July, 5, 1990) states that NSA is the national manager for "National Security Systems" and is responsible to:

> a. Examine U.S. Government national security systems and evaluate their vulnerability to foreign interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Order and implementing procedures, and applicable Presidential directive. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned;
>
> b. Act as the U.S. Government focal point for cryptography, telecommunications systems security, and information systems security for national security systems;
>
> c. Conduct, approve, or endorse research and development of techniques and equipment to secure national security systems;
>
> d. Review and approve all standards, techniques, systems, and equipment related to the security of national security systems;
>
> e. Conduct foreign computer security and communications security liaison, including entering into agreements with foreign governments and with international and private organizations regarding national security systems, except for those foreign intelligence relationships conducted for intelligence purposes by the Director of Central Intelligence. Any such agreements shall be coordinated with affected departments and agencies;
>
> f. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provisions of cryptographic and other technical security material or services;
>
> g. Assess the overall security posture of and disseminate information on threats to and vulnerabilities of national security systems;

> h. Operate a central technical center to evaluate and certify the security of national security telecommunications and information systems;
>
> i. Prescribe the minimum standards, methods and procedures for protecting cryptographic and other technical security material, techniques, and information related to national security systems;
>
> j. Review and assess annually the national security telecommunications systems security programs and budgets of Executive departments and agencies of the U.S. Government, and recommend alternatives, where appropriate, for the Executive Agent;
>
> k. Review annually the aggregated national security information systems security program and budget recommendations of the Executive departments and agencies of the U.S. Government for the Executive Agent;
>
> l. Request from the heads of Executive departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned herein;
>
> m. Coordinate with the National Institute for Standards and Technology in accordance with the provisions of the Computer Security Act of 1987 (P.L. 100-235); and
>
> n. Enter into agreements for the procurement of technical-security material and other equipment, and their provision to Executive departments and agencies, where appropriate, to government contractors, and foreign governments. (NSD-42, 1990, para. 7)

Beyond the simple title designation, the above clearly reiterated numerous times are the various duties associated with protection of national security systems. This makes the defense of national security systems plainly in the realm of NSA's mandate. By maintaining this cyber capability, it also allows the DHS to utilize those same services, when needed in response to a CI/KR cyber-attack or intrusion, per the Economy Act of 1932 (Pub. Law No. 72–212; 47 Stat. 382) and Disaster Relief Act of 1974 (Public Law No. 93–288), as amended by the Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988.

c. NSA Efforts

The NSA maintains relative confidentiality on its capabilities and thus this section is truncated due to classification restrictions. This should not be a surprise, as initially noted in the Limitations section of Chapter 1, due to the highly classified nature of the cyber capabilities, little in the way of capabilities will be delved into in an effort to keep the propensity of this thesis at the lowest level of classification possible. As such, it will be grossly assumed that DoD, and by subordination NSA, by the very nature of training, billets, commands, and funding has the necessary means to employ and/or build the requisite capabilities needed to exercise its authorities in the cyber domain.

What is important to note is that the NSA, as a subordinate agency to the DoD, has been the site of colocation and dual hatting of the commander of DoD's USCYBERCOM. What this enables is a breadth of operational capability with a growing organization trying to build those capabilities for offensive use. Although significant public discussion continues with regard to the validity of the pairing, it nonetheless is the reality at the time of this thesis. It is also important to note that each has differing statutory authorities, but are positioned for synergistic efforts when needed.

2. Central Intelligence Agency

The CIA plays an integral role in the protection of national CI/KR in a limited sense. Due to their mandate, they have no internal security functions and therefore have no legal enforcement powers domestically. As such, their direction, deconfliction, and use of human intelligence (HUMINT) sources is essential in gaining access to personnel or networks, which need to be exploited for valuable information and intelligence and would otherwise be inaccessible.

a. CIA Authorities

Pursuant to Title 50, the CIA has the responsibility to:

> (1) collect intelligence through human sources and by other appropriate means, except that the Director of the Central Intelligence Agency shall have no police, subpoena, or law enforcement powers or internal security functions;

> (2) correlate and evaluate intelligence related to the national security and provide appropriate dissemination of such intelligence;
>
> (3) provide overall direction for and coordination of the collection of national intelligence outside the United States through human sources by elements of the intelligence community authorized to undertake such collection and, in coordination with other departments, agencies, or elements of the United States Government which are authorized to undertake such collection, ensure that the most effective use is made of resources and that appropriate account is taken of the risks to the United States and those involved in such collection; and
>
> (4) perform such other functions and duties related to intelligence affecting the national security as the President or the Director of National Intelligence may direct. (50 U.S.C. §403–4a, sect. d)

This is significant as it establishes the CIA as the primary agency with statutory authority for HUMINT, as well as assigning it analytical functions. Primarily due to the above clause negating internal security functions, much of the intelligence collection of the CIA is directly governed by the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §1801 et seq.).

b. CIA Role

Executive Order 13,470 (July 30, 2008) amended Executive Order 12,333 (December 4, 1981) to include the responsibilities of the CIA. The amended EO states that the CIA shall:

> (1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;
>
> (2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;
>
> (3) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;
>
> (4) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any

period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93‑148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;

(5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;

(6) Under the direction and guidance of the Director [DNI], and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and

(7) Perform such other functions and duties related to intelligence as the Director [DNI] may direct. (Executive Order No. 12,333, as amended 2008, para. 1.7(a))

c. CIA Efforts

The CIA also maintains relative confidentiality on its capabilities and thus this section is truncated due to classification restrictions. What is important to note is that their capabilities may be leveraged by other agencies when deemed operationally necessary and as deconflicted by the DNI.

I. CHAPTER SUMMARY

This chapter has undoubtedly been the most difficult to compile due to the various competing sources available and attempts to restrict the discussion to that involving authorities, roles, and efforts with respect to cybersecurity of CI/KR. It has outlined the majority of authorities as provided in the U.S. Constitution and U.S. Code for each of the respective major areas involving the cybersecurity of national CI/KR. Below is the analysis of organizations and/or agencies identified above, with respect to the required authorities to carry out their respective roles in achieving the National Preparedness Goal.

What this chapter has failed to do is show significant synergy between the involved executive agencies and private sector in order to proactively mitigate national CI/KR incidents from a cybersecurity standpoint. The bi-lateral agreement between the

DHS and DoD represents an exception to this overall trend. As the effort extends beyond simply two executive agencies, this highlights a deficiency. Beyond the recently generated OUSD-P Bubble Chart of the U.S. Federal Cybersecurity Operations Team (Figure 4), which is a graphic depiction of notional roles and responsibilities, the lines are still blurred or in need of updating. This regresses back to the much anticipated National Protection Framework and the expectation that it will better define those roles and responsibilities as worked on by the various representatives of those executive agencies. As this will be addressed in the following chapter, below is the analysis of the authorities from each section provided in this chapter.

1. DHS

The authorities aligned under the DHS are reactionary in nature and thus assume a response and recovery role post INS designation.

This approach, predicated from the fact that the DHS is an executive agency created of consolidated authorities to primarily address the response to domestic terrorism, assumes that the U.S. will continue to focus on post-event triage and coordination vice pre-event mitigation. Without a revision of these authorities and mandates for the DHS, it is clear that the federal government of the U.S. is missing an opportunity to assist the private sector in the common cause of protecting the national CI/KR.

As such, this continues to discount the importance of the indicators that the private sector and various federal agencies could provide in advance to an attack on national CI/KR. Although information sharing can be accomplished (often in sanitized form) from the federal government via the DHS NCCIC (utilizing statutory authorities as provided via the Homeland Security Act of 2002), there are insufficient laws in place to protect private sector liability issues for sharing their indications and warnings proactively and thereby aid to paint a larger picture of the national cybersecurity posture for CI/KR.

To further complicate this, although authorized to share the indications and warnings (e.g., NSA via SIGINT, CIA via HUMINT, DoD by nature of protecting the

GIG/DIB, or FBI by means of an ongoing investigation) of a significant malicious event being planned for future execution, there apparently is no mandated requirement to. Without the clear knowledge that lives are in danger, the concern is that information sharing is still restrictive as each agency is likely to protect their various intelligence sources and methods and are in no way are compelled to share the information if imminence or credibility are less than certain. This highlights a limiting factor of the DHS mandate to protect the nation, as their analysis will only be as good as the information provided by which to analyze.

Further highlighting this deficiency, written testimony of NPPD Office of Cybersecurity & Communications Acting Assistant Secretary Roberta Stempfley, and National Cybersecurity and Communications Integration Center Director Larry Zelvin for a House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies hearing documents titled *Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities* states:

> … The U.S. national strategy for responding to cyber threats to CI/KR is deficient because it lacks provisions for the federal government to immediately (1) assess current or cascading damage to CI/KR and (2) assess corresponding needs of essential services for affected victims, when needs outweigh the resources of the state, local, and private voluntary community. Moreover, the U.S. national strategy—encompassing 30(+) different agencies—does not promote adequate preparedness when there is advance warning of a disaster because preparatory activities are not explicitly authorized until the President has issued a disaster declaration. (Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities, 2013)

Therefore, although DHS is working to establish situational awareness by building the common operational picture (COP) for the federal civilian agencies, it will eventually need to be blended with the DoD operational picture of the GIG and DIB, as well as allowing for expansion for public and private sector participation/feeds, if a whole-of-nation approach is ever to be achieved. Therefore, instead of creating a COP that would be technologically unviable to connect with, through the evolving standards of

the National Institute of Standards and Technology (NIST), it stands to reason that we could leverage the NIST's significant expertise to work the issue on our behalf. This idea is not entirely original, as a congressional hearing on the "Oversight of Executive Order 13636 and Development of the Cybersecurity Framework" was held on July 18, 2013 and the idea of allowing NIST to propose the national cybersecurity framework was reinforced by Dr. Eric A. Fischer, Senior Specialist in Science and Technology for the Congressional Research Service. As this recommendation already appears to be fielded for action and oversight, mentioning it as a recommendation in this thesis is unnecessary. As such, I applaud that idea has already been socialized, by leveraging the subject matter experts of their respective fields to study and propose viable solutions which are palatable and easily understood by the private and public sector companies concerned, as it appears to be the smartest way to proceed.

2. DoD

Sufficient authorities exist in Title 10 for the DoD to execute its intended mission of defending the nation when an aggressor is identified.

3. DOJ

Sufficient authorities exist in Title 18 for the DOJ to enforce, and investigate violations of, federal laws. Expansion and/or clarification of those laws, however, will continue to be necessary as societal and international norms highlight deficiencies in current protection. Current failure of U.S. law to adequately provide liability protection for private sector companies impedes the national efforts. This oversight precludes timely information being provided to the federal government, ideally through the NCCIC, in order to meet the goal stated in the Critical Infrastructures Protection Act of 2001.

4. National Guard

Sufficient authorities exist in Title 32 for the National Guard to execute its intended mission of planning, preparing, and responding to natural or manmade incidents at the state and federal level. This is a force of augmentation for the response and recovery mission areas of the National Planning System.

5. Public Building, Properties and Works

Sufficient authorities exist in Title 40 for the safeguarding of public buildings, properties and works. With respect to the information procurement though, there exists and opportunity to reduce the number of dissimilar devices employed. Although possibly to be resolved in acquisition reform and not exactly Title 40, standardization of information systems in the federal agencies would have pros and cons. Although it would likely create a monopoly for the chosen providers and singular target for hostile entities, it would also minimize the sheer number of differing edge devices requiring management and patching, thereby reducing the cybersecurity burden.

6. National Policy for CI/KR Protection

Sufficient authorities exist in Title 42 for clarification of the current national policy with respect to response and recovery from cyber-attacks or intrusions into national CI/KR. What is lacking is the coordination with the national intent to minimize unnecessary damage by proactively addressing the prevention, protection, and mitigation aspects as outlined in PPD-8.

7. Public Printing and Documents

Sufficient authorities exist in Title 44 for the executive agencies to designate a CIO, whom enforces mandated federal information policies contained therein. Statutory authorities should be revisited, however, with the failed *Protecting Cyberspace as a National Asset Act of 2010* (Senate Report No. 111-368) as a template to increase justification of the E^3A upgrade by the Network Security Deployment branch of the DHS NPPD.

8. Intelligence Community

Sufficient authorities exist in Title 50 for the executive agencies to support cybersecurity protection of national CI/KR through intelligence collection, activities and covert action.

As it stands given the existing U.S. Code, the authorities and roles are appropriate to achieve a whole-of-nation approach to response and recovery from a cyber-attack on our national CI/KR. The perceived intent, however, is that effective national cyberstrategy exceeds this narrow focus and actually prevents, protects, and mitigates threats.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ANALYSIS

What I have found are areas for improvement, but no silver bullets that would specifically support that a unity of command approach would be a significantly better approach to protecting our nation's CI/KR from cybersecurity threats. While involving multiple agencies in the unity of effort approach unquestioningly creates bureaucratic delay in execution, the unity of effort currently appears to be a necessary evil, as no single agency has the authority, or mandate, to handle all aspects of the active and passive responsibilities involved in protecting the nation's CI/KR. This comes at a point in time when serious concerns are being raised as to the alleged privacy abuses of federal agencies entrusted with our protection (e.g., warrantless wiretapping by the NSA) (Landau, 2013, p. 56). This point, combined with the significant reluctance of the U.S. public to set aside previously disclosed federal abuses of civil rights and privacy, significantly reaffirms the current unity of effort approach.

A. ANALYSIS

Documented previously, efforts of the last three U.S. presidents (from 1996 to present) to address protecting national CI from cyber threats seem circular in nature as each new presidential administration in the last 17 years: (1) identifies a critical vulnerability in the national defense of critical infrastructure, (2) creates a committee of experts and insiders to research and evaluate issues, and then (3) implements a personalized unity of effort strategy.

DHS currently has the assigned responsibility to protect the nation and provide analysis, warning, and technical support to critical infrastructure, which equates to being the lead for centralized planning of the decentralized execution of the security of cyberspace of the nation (Homeland Security Presidential Directive 7, 2003). The cyber-role of DoD centers on defending the GIG and DIB, providing signatures of cyber threats gained by classified means, and support to DHS efforts upon request to provide intelligence and attribution support. To fill these roles, in the last four years, DoD has made progress by establishing U.S. Cyber Command and service-specific cyber

commands/elements (GAO Testimony 11–865T, 2011). Additionally, as recently as the past year, DoD has begun to standardize and define key terminology and recognized the need to develop and update cyber-related joint doctrine, possibly through the development and publication of a single cyberspace operations joint doctrine publication (GAO Report 11–75, 2011). As such, these efforts highlight the utility of the various federal agencies and their dedication to the unity of effort approach. These efforts are laudable but gaps remain between the stated intent contained within policy and execution.

1. Identified Gaps

There are sufficient authorities in place to execute a federal response to the violation of national integrity of information systems connected to and controlling U.S. CI/KR, as executed through the cyber operational domain. What seems to be lacking is the updated national guidance with sufficient authorities and laws to prevent, protect against and mitigate unnecessary damage to national CI/KR from cyber-attacks in the first place.

a. Documents

Despite not being able to read every single document produced or released on the topics of cybersecurity or critical infrastructure protection, I have been able to identify some issues with existing documentation.

(1) Title 42. The Critical Infrastructures Protection Act of 2001 states that the official U.S. policy is that "… any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States" (42 U.S.C. 5195c, sect. c(1)). This is a reactionary policy with embedded goals for CI/KR protection criteria. Unfortunately, this codified U.S. policy is at odds with the decade newer guidance released as the National Preparedness Goal, directed by PPD-8: "A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk" (National Preparedness Goal, 2011, p. 1). The disparity lies in that Title

42 addresses and focuses solely on post-event criterion, whereas the national preparedness goal covers a broader spectrum of preparedness which incorporates prevention and protection, preemptive of an INS. Therefore, Title 42 of U.S. Code needs to be updated to match the current CI/KR protection policy.

(2) Lexicon Standardization. Although the CIP policy still comes from the older U.S. Code, the genesis of the current national strategy to protect U.S. CI/KR comes from the guidance in PPD-8, National Preparedness Goal, and National Planning System. These documents do one key thing of note. PPD-8 calls for an all-of-nation approach (implementation of the unity of effort concept), utilizing the greater inclusivity implied by the term to highlight the contributions necessary by the private and public sectors to reach the collective end-state. This is a clear deviation from previous documents, which call for a whole-of-government or federal approach. These other terms previously, and likely unwittingly, discounted the private and public sector contributions required to be effective, even after frequently including them in documents. Although editing every historic document to standardize the lexicon is unwise, as documents are renewed, reviewed and/or updated, they should make every attempt to use the terms uniformly.

(3) Revise SNRA Threshold Criteria. Additionally, addressed in the SNRA mandated by the National Preparedness System, identification of the cyber-attack threshold is useful but precluded by the difficulty in definitively calculating monetarily defined effects post cyber-attack, in order to assess the damage in relation to the significant thresholds to meet the national-level event criteria.

(4) National Protection Framework. The National Planning System is still a work in progress as it attempts to address the mandates set forth in PPD-8; the DHS is still attempting to produce, deconflict, and disseminate all five interdependent national planning frameworks. The specific delay, however, in the National Protection Framework has created a void in known roles and responsibilities for the core capability of cybersecurity, which must be rectified quickly. Without the stated guidance that this document is anticipated to provide from the national level, the direct justification for many of the U.S. cybersecurity efforts is lacking. Prior to its approval

and dissemination by the DHS though, it needs to be socialized with the respective executive agencies representatives, whom have already been deconflicting roles and responsibilities for the federal cybersecurity mission (e.g., OUSD-P Cyber). Regardless, this continued delay is directly incongruent with President Obama's guidance provided over four years ago on May 29, 2009 in which he stated:

> From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage. (Obama, 2009, p. 4)

This sub-section arguably could have also been in the following responsibilities section, but as the document itself is missing and unavailable for review, it has been placed in initially in the document section, with additional comments in the responsibility section. Without reviewing the document, there is no constructive commentary to be provided to assist in its completion.

b. Responsibilities

The National Protection Framework, as a subcategory of the National Planning System, is the primary national document that is supposed to provide a "… detailed concept of operations; a description of critical tasks and responsibilities; detailed resource, personnel, and sourcing requirements; and specific provisions for the delivery of capabilities … by the Federal Government" (National Preparedness System, 2011, p. 4). Due to its previously noted absence, the attempted research on nationally dictated responsibilities with respect to CI/KR was essentially null and void as the majority of findings will need to be immediately reassessed against the National Protection Framework as soon as it is released. An exception to this lack of national responsibilities comes from the designation of the DHS as the cybersecurity lead, which requires a degree of situational awareness.

(1) Cybersecurity Situational Awareness. Without guidance of the National Planning System, the DHS is obligated, via the expectation to implement the National Preparedness Goal, to prevent, protect against, and mitigate threats to the

otherwise secure and resilient national CI/KR (as the lead for both cybersecurity and CI/KR protection). How then can they be expected to do this for the cybersecurity discipline when the majority of CI/KR is developed, operated, and owned by the private and public sectors? Any proficient system administrator or CIO will say that they, the DHS, cannot. Without interconnected feeds to a situational awareness tool for analysis, such as a common operational picture, this preempts that ability. EINSTEIN may provide federal civilian information system indicators, and DoD may provide federal government information system indicators, but if readiness requires fusion with the private sector companies in charge of CI/KR, how then can the DHS provide timely and accurate assessment of the health of the nation's cybersecurity? I submit, at the risk of appearing overly repetitive, that they cannot. More importantly, how can those responsible for assessing ongoing cyber-attacks and current malicious cyber activity accurately advise the U.S. president or NORTHCOM commander as to the current scope of the threat posed to the nation? Although effort and progress is being made by the DHS and like-minded partners (e.g., NIST), the creation of a solution is still evolving. This creates a disparity between an unrealistic expectation of capability in maintaining situational awareness and the requirement for the NORTHCOM commander to be able to make informed assessments which could affect the national defensive posture.

Understanding that significant legal liability impediments and a dearth of strict regulations preclude the proactive cyber-intelligence sharing by the private and public sectors, this creates a gap between desired outcome and regulatory required behavior.

c. Authorities

Previously highlighted, the authorities, aligned under the DHS as the lead for cybersecurity, are reactionary in nature and thus assume a response and recovery role post INS designation while failing to emphasize the usefulness of prevention, protection, and mitigation. This does not exactly translate into a deficiency, but rather into a matter of evolution. The DHS, to now achieve the stated national preparedness goal, requires

broader statutory authority to address the proactive aspect of domestic security, as repetitively mentioned earlier.

Unexpectedly during my research, it was discovered that a high visibility cyber-related issue of national concern could possibly be mitigated by simple revision of existing wording in Title 6 of the U.S. Code. This revision would formally provide the DHS with the necessary statutory authority to specifically take the lead on intellectual property theft being perpetrated through the cyber domain. Current law, created over a decade ago when the DHS was being established, states that the DHS will "… ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland…" (6 U.S.C. §111, sect. 101, para. b.1.F). Through minor edits, this subparagraph could easily be modified in one of two ways: (1) that the DHS will "… ensure that the overall economic security of the United States is not diminished by [*malicious*] efforts, activities, and programs [*initiated or controlled by aggressors utilizing the cyber domain*] …."; or (2) that the DHS will "… ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland, [*nor allow it to be diminished by malicious efforts, activities, and programs initiated or controlled by aggressors utilizing the cyber domain*] …." Not only would either of these proposed revisions cover dedicated efforts of major intellectual property theft, but either is broad enough to account for any future cyber-related threat to U.S. economic security. This is not to say that they pre-empt the DOJ in their federal law enforcement role, but it would clearly set the standard of providing the DHS with the statutory authority to specifically be looking for those crimes in order to alert the DOJ. As this is not solely for the protection of CI/KR, and would cause significant outcry from industry, I have refrained from including this in the recommendations given in the next chapter.

VI. CONCLUSION, RECOMMENDATIONS AND FUTURE WORK

Building from the analysis by which gaps were identified this chapter begins with my conclusions, proposes recommendations to close the gaps and concludes with recommendations for future work.

A. CONCLUSION

In conclusion, this thesis has examined the current and past literature involving CIP and emergency response by reviewing the various roles and authorities allocated to the major federal agencies. In summary of the analysis, the U.S. has experienced numerous strategy assessments, with respect to cybersecurity of the national CI/KR. This spiral is fixed in place primarily due to the continual realization that there exists a clear disparity between the strategic national requirements and DHS' execution of their mandate regarding the protection of CI/KR and emergency management. To be more specific, the DHS is mandated to protect national CI/KR, but only given authority and responsibility to respond and recover to INS post occurrence. This incongruence between that stated strategic national goal and the needed prevention, protection and mitigation aspects of regulatory guidance and authorities is evident by the strategy assessment spiral.

Although not necessarily palatable, the specific recommendations with respect to improving the cybersecurity of the national CI/KR, are to:

- Update the U.S. National Policy on CI/KR Protection;
- Update the U.S. National Cybersecurity Strategy;
- Ensure the National Protection Framework Includes Clear and Deconflicted Roles and Responsibilities for Cybersecurity;
- Expand/Revise DHS Authorities;
- Revisit Cyber-attack Threshold Criteria Used in the SNRA;

- Standardize Lexicon;
- Incentivize Private Sector Participation in a CI/KR COP; and
- Provide Liability Protection for Private Sector Voluntary Information Sharing.

Cyber-related threats are an ever-developing and increasing part of the nation's vulnerability and the homeland security enterprise must be a part of this evolutionary solution or they will fail. This thesis is provided as a basic background of the authorities and responsibilities associated with CI/KR protection and their alignment with U.S. strategic intent. Common sense must eventually prevail; the question remains if it is to be through reason or through the experience granted over time.

B. RECOMMENDATIONS

Three key points not covered by this research must be conceded to move forward: (1) the U.S. maintains one of the most powerful militaries in the world; (2) globalization has interconnected many politically divergent economies; and (3) social networking has created communities beyond the national identity. These three points, when combined, lend themselves to highlight that the most likely threat to the U.S. is via an asymmetric vector where attribution is difficult and threat of escalation is low. One such asymmetric vector that aligns with these criteria is a cyber-attack. Whether conventional or asymmetric, any dedicated force with the means will attempt to reduce uncertainty and risk by conducting reconnaissance prior to initiating an attack. This specific premise is reinforced when the cyber-attack on Estonia in 2007 is reviewed. Therefore, cyber intrusions into U.S. systems, whether CI/KR or not, are likely to be significant indicators that can assist the U.S. government and, by extension, the DHS and DoD to assess aggressor intent. To break into aggressors' operational and informational cycles earlier than after execution, the U.S. needs to address the following recommendations.

1. Update the U.S. National Policy on CI/KR Protection

The DoD teaches its officers that all efforts begin with, and are defined by, requirements. Why is it then that U.S. policy for critical infrastructure protection in U.S.

Code (42 U.S.C. 5195c, sect. c(1)) is still dated from 2001 and has yet to be updated to match the broader 2011 National Preparedness Goal two years after the fact?

Update Title 42 to include the prevention, protection, and mitigation aspects of preparedness necessary to justify proactive critical infrastructure protection, in addition to the reactionary ones currently alluded to—response and recovery.

2. Update the U.S. National Cybersecurity Strategy

Much like the findings published in December 2008 and reiterated in their 2011 report, the Commission on Securing Cyberspace for the 44th Presidency highlight that a revision of the national cybersecurity strategy is immediately necessary (Securing Cyberspace for the 44th Presidency, 2008, p. 1; Cybersecurity Two Years Later; 2011, p. 5). As I have waded through significant volumes of policy, authority and miscellaneous departmental documents, I concur. Many executive agencies have published their individual cyber strategies, but I find it difficult to fathom how they are aligned, if not under a single current national cybersecurity strategy. In order to better align the common desired end-state, the National Strategy to Secure Cyberspace (2003) needs to be updated.

As such, the updated national cybersecurity strategy should be nested under the National Planning System. This document should be created through the updating and minor revision of three existing documents as templates—National Strategy to Secure Cyberspace, Comprehensive National Cybersecurity Initiative, and PPD-8—with specific emphasis on three key issues: (1) utilization of a whole-of-nation approach; (2) addressing all five national preparedness mission areas; and (3) broadening of threat categories to be all-inclusive at a national level. Due to the desired nested nature of the national cybersecurity strategy as a strategic document, I recommend that both PPD-8 and the National Planning System be preemptively updated to reflect their national focus, vice their current focus on the specific threats posed by terrorism and disasters.

a. PPD-8 and National Planning System

PPD-8, and by default the National Planning System, set a significant precedence of a national preparedness standard by which national agencies could unify toward a common goal. The issue identified is that the National Preparedness Goal provided by PPD-8 focuses too narrowly on terrorism and disasters. They were clearly written by the DHS for DHS while posing as national level documents. This should have never been an acceptable answer to national preparedness and needs to be rectified to reflect President Obama's stated intent.

Additionally, while not seeking this conclusion in this research, incidental findings indicate that current national preparedness documents makes no allowance for espionage, industrial or otherwise, as they have too narrow of a focus. I submit that, when developed, a sound national cybersecurity strategy is a prerequisite to achieving preparedness.

This gap in strategic intent and practice has allowed for an unprecedented theft of U.S. intellectual property, which is clearly in the DOJ's standing mandate to impede as a violation of federal law.

3. Ensure the Pending National Protection Framework Includes Clear and Deconflicted Roles and Responsibilities for Cybersecurity

Although the recommendation title is fairly clear, it should be noted that work has already been done on this front by OUSD-P Cyber, DHS, and DOJ through their interagency efforts to create the Bubble Chart (Figure 4). Failure to include this graphic in current or updated form, or more importantly a significant written explanation of the graphically depicted duties, would draw significant suspicion as to validity and actual cooperation and deconfliction between the executive agencies.

4. Expand/Revise DHS Authorities

The national CI/KR is a system of systems. This concept should not be lost on the reader. Cybersecurity, as a commercially lucrative discipline, has already been addressing this problem and I believe can be used to illuminate the way ahead.

When securing a system it is logical to start with the basics, which are local security measures, both physical and logical. As the system grows or security needs to be heightened, the logical progression is to install an IDS to detect known signatures or behaviors that put the system at risk. This is eventually followed by the upgrade to an IPS, which adds automatic system configuration responses to mitigate incoming rule-based undesired traffic.

The DHS is monitoring the executive agencies for anomalies at an improved IDS level, while apparently waiting for authorization to upgrade to the IPS functionality offered by E^3A. Two routes present themselves, but the least effort would be to revisit statutory authorities in Title 44, with the failed *Protecting Cyberspace as a National Asset Act of 2010* (Senate Report No. 111-368) as a template to increase justification of the E^3A upgrade by the Network Security Deployment branch of the DHS NPPD.

5. Revisit Cyber-attack Threshold Criteria Used in the SNRA

Although addressed in the SNRA, identification of the cyber-attack threshold criteria is useful but precluded by: the difficulty in definitively calculating monetarily defined effects post cyber-attack, in order to assess the damage in relation to the significant thresholds to meet the national-level event criteria. To be honest, although I recommend revisiting this criterion for revision and clarification, I believe significant study and analysis should be done due to the seriousness and sensitivity of the topic. I therefore will include this as a topic for additional research in my future work section.

6. Standardize Lexicon

Clouding the issue of effective cybersecurity is the loose use of non-standardized terminology. The DoD has attempted to standardize its internal lexicon, but sometimes at the exclusion of terms already commonly used in private industry (e.g., cyber-attack as defined by CNSSI/NIST). Although the DoD does this to more clearly justify operations under authorities provided, it may perpetuate unintentional miscommunication. The claim that a military unit suffered a cyber-attack may mean something very different than if private-sector company issued the same claim. I propose that we start with standardizing two key terms—cyber-attack and whole-of-nation.

a. Cyber-attack

Although the official definition of cyber-attack remains a matter of contention, the threshold of what constitutes an INS is not. The Strategic National Risk Assessment (2011) defines specific INS attack thresholds for cyber-attacks on both data and physical infrastructure in terms of thresholds for only integrity and availability. The term cyber-attack is not defined internal to the SNRA, but rather it is used in defining the INS attack thresholds. This may create uncertainty with respect to evaluating those explicitly stated INS thresholds, as the NIST definition also appears to include confidentiality. This is not to say that a confidentiality threshold was not considered when writing the SNRA, but logically may have been excluded intentionally in favor of maintaining the focus on the two aspects which directly affect proper operation of national CI/KR.

This distinction, and consistent use of a standardized cyber-attack term, is important. To resolve the contention over the term cyber-attack requires that all federal agencies agree on whether it includes operations that compromise confidentiality; that is, whether a cyber-attack includes "… stealing controlled information" (Glossary of Key Information Security Terms, 2013, p. 57; Committee on National Security Systems Instruction 4009, 2010, p. 22). Specifically, clear delineation is important for the DHS, NORTHCOM commander and USCYBERCOM to justify an assessment that the nation is under attack, via the cyber domain, to the President.

This clarification may prompt additional discussion as to whether theft of controlled information can ever reach a threshold to be considered an INS, thereby invoking a national response, or if it should be specifically discussed in future revision of the national cyber strategy. The scope of this recommendation, and factors for consideration, justifies careful consideration. As such, it has also been included in the future work section.

b. Whole-of-Nation

Cybersecurity of the national CI/KR is not solely a federal, state and local government issue. Why then do so many of the documents use the term whole-of-

government or federal approach? All are examples of a unity of effort implementation, but these terms automatically discount the contributions required by the private and public sectors by creating the misperception that the government alone can provide the cybersecurity necessary to better safeguard the CI/KR sectors. As such, references should be reviewed for exclusive terminology and be replaced with inclusive terms, which more accurately encompass the focus on the national effort and contributions of the public and private sectors. I propose use of the term *whole-of-nation*. Just think, with implementation of the whole-of-nation (WoN) approach, we have already "WoN."

7. Incentivize Private Sector Participation in a CI/KR COP

Regulatory mandate is often seen as the compulsory method to force private sector compliance with much needed reforms for the good of the nation. In fact, both reports from the Commission on Securing Cyberspace for the 44th Presidency (2008 & 2011) recommended that the federal government regulate cyberspace as a mandatory milestone to achieve acceptable levels of cybersecurity (Securing Cyberspace for the 44th Presidency, 2008, p. 2; Cybersecurity Two Years Later; 2011, p. 1). I submit that, although practical, a second approach may be more palatable and therefore should be better analyzed—incentivization. This proposes the carrot over the stick.

Regulation of federal and state systems seems prudent, as presented in Title 44, but general regulatory changes for the private and public sector may not be necessary if sufficient incentives are provided to voluntarily participate. This solution seems preferable as the private-sector is already burdened with various compliance requirements, and is therefore unlikely to willingly assume others unless there is significant return on investment. That is not to say that the federal government should over regulate or assume the sole protection of national CI/KR. On the contrary, by creating a system by which a COP is voluntarily opted into through the automatic and encrypted feeds from the disparate private sectors responsible for CI/KR, additional regulation forcing the private and public sector participation may become unnecessary. This is in direct conflict with the report by the Commission on Securing Cyberspace for

the 44th Presidency as they state "… voluntary action is not enough" (Securing Cyberspace for the 44th Presidency, 2008, p. 2).

In looking at this recommendation, it should be assumed that in the interest of profits, that private sector companies utilize some form of network protection and thus maintain a means of localized compiling and logging of anomalies. The U.S. government should then capitalize on their efforts and offer opted-in companies the expertise, if not hardware, necessary to connect the private security information and event management (SIEM) systems to the national CI/KR COP. This would defer cost to the federal government and ease any perceived burden on the private sector. Actual incentives for the program should be seriously considered, but could include free sharing of nationally collected threat signatures from the Enhanced Cybersecurity Services offered by DHS and/or a public association with the national effort to secure the U.S. CI/KR, thereby increasing public confidence in continuity of services. It is important that these incentives be logically significant enough to offset any reservations that public or private companies would have regarding the information sharing agreement. It would be remiss to not note that the companies may incur a significant challenge as privacy advocates would raise concerns about the additional sharing of data with the government. Their concerns carry more weight in light of the recent alleged NSA abuses as revealed through former employees, and as cries are heard to the effect that "…limiting government's power is fundamental to the US political system" (Landau, 2013, p. 55).

8. Provide Liability Protection for Private Sector Voluntary Information Sharing

Current failure of U.S. law to adequately provide liability protection for private sector companies impedes the national efforts. This oversight precludes timely information being provided to the federal government, ideally through the NCCIC, in order to meet the goal stated in the Critical Infrastructures Protection Act of 2001. Although lexicon standardization has been an impediment to previous attempts to introduce legislation which would provide this (e.g., Critical Intelligence Sharing and Protection Act), scope of the bill should be narrowed, and reduction of ambiguity should be sought in providing a definition section, in order to expedite the passing of this crucial

piece of legislation. It should also be clear that the federal government is to receive processed cyber intelligence and indicators (e.g., externals) of communications and not raw U.S. person data (e.g., internals) unless required by U.S. law to an agency authorized to obtain such data, in accordance with existing laws.

C. SUGGESTED FUTURE WORK/RESEARCH

Due to the complex nature of the emerging and increasing vulnerability combined with the interdependencies in both technology and authorities, the topic of the protection of national CI/KR from cyber-threats is a broad field ripe for continued/future work.

Primary suggestions for future research are: (1) comparison of the U.S. national roles and responsibilities with other western nations (e.g., United Kingdom, Australia, Canada, New Zealand, Denmark, and Norway); (2) research into the inclusion or continued exclusion of confidentiality in the threshold definition of a cyber-attack; (3) the policy, legal (to include regulatory) and financial security issues that would need to be resolved to better integrate the private sector for a whole-of-nation response in CI/KR protection; (4) an analysis of the DIB perimeter, with a focus on DoD's responsibility as the SSA; (5) privatization, with respect to the government's ability to establish and maintain control of national security initiatives; and (6) the national strategic implications relative to the political and economic issues, both positive and negative, for military involvement in cyber defense of non-DoD critical infrastructure.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Bacon, F. (1597) Of heresies; Meditationes sacrae (1597), Chapter 11; M5.

Breen, M., & Geltzer, J. (2011). Asymmetric strategies as strategies of the strong. *Parameters*, 41(1), 41–55. Retrieved from ProQuest database: http://search.proquest.com/docview/886828350?accountid=12702

Cabana, N. (2000). Cyber attack response: The military in a support role. *Air & Space Power Journal* (04 April 2000). Retrieved December 07, 2011, from web: http://www.airpower.maxwell.af.mil/airchronicles/cc/cabana.html

Central Intelligence Agency (1999). *A consumer's guide to intelligence*, Washington, DC: Central Intelligence Agency, 1999, vii.

Coakley, T. P. (1991). *Command and control for war and peace.* Washington, DC: Diane Publishing, 75.

Comprehensive national cybersecurity initiative (2008). Washington, DC: Government Printing Office. (Jan 2008). Retrieved June 10, 2013 via Whitehouse CNCI main page: http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

Congressional Record. (2000). Statement for the record of NSA director Lt Gen Michael V. Hayden, USAF; House Permanent Select Committee on Intelligence. (17 April 2000). Retrieved January 23, 2013 from NSA Main Page via web: http://www.nsa.gov/public_info/speeches_testimonies/12apr00_dirnsa.shtml

Critical foundations: Protecting America's infrastructures. (1997). Report of the President's Commission on Critical Infrastructure Protection. Washington, DC: Government Printing Office, (1997). Retrieved April 16, 2013 from the web via http://www.fas.org/sgp/library/pccip.pdf

Critical infrastructure and key resources support annex. (2008). National Response Framework (1st Ed.). (2008). Department of Homeland Security. Washington, DC: Government Printing Office. (Jan 2008). Retrieved June 10, 2013 from Homeland Security Digital Library: https://www.hsdl.org/?view&did=483067

Cybersecurity two years later. (2011, January). Commission on Cybersecurity for the 44th Presidency; Center for Strategic and International Studies; Washington D.C. Retrieved April 24, 2013 from CSIS Digital Library: http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf

Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure (2009). Washington, DC: Government Printing Office, (May 2009). Retrieved May 5, 2012 from Whitehouse Main Page via web http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Dobitz, K., Hass, B., Holtje, M., Jokerst, A., Ochsner, G., & Silva, S. (2008). The Characterization and Measurement of Cyber Warfare. U.S. Strategic Command: Global Innovation and Strategy Center (Project 08–01). Retrieved from DTIC database: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA497907

Economy Act of 1932, as amended. Pub. L. No. 72–212, 47 Stat. 382 (June 30, 1932), 31 U.S.C. §1535. *U.S. House of Representatives*, 72nd Cong. (1932).

Executive Order No. 12,127, 44 FR 19,367 (April 3, 1979), 3 C.F.R. (1979 comp.), p. 376.

Executive Order No. 12,148, 44 FR 43,239 (July 24, 1979), 3 C.F.R. (1979 comp.), p. 412

Executive Order No. 12,333, 46 FR 59,941 (December 8, 1981), 3 C.F.R. 200 (1981 comp.)

Executive Order No. 12,381, 47 FR 39,795 (September 10, 1982), 3 C.F.R. (1982 comp.)

Executive Order No. 12,656, 53 FR 47,491 (November 23, 1988), 2 C.F.R. (1988 comp.)

Executive Order No. 12,673, 54 FR 12,571 (March 28, 1989), 2 C.F.R. (1989 comp.), p. 214.

Executive Order No. 12,803, 57 FR 19,063 (May 4, 1992), 20 C.F.R. 111 (1992 comp.)

Executive Order No. 13,010, 61 FR 37,347 (July 17, 1996), 3 C.F.R. 333 (1996 comp.)

Executive Order No. 13,130, 64 FR 38,535 (July 19, 1999), 3 C.F.R. (1999 comp.)

Executive Order No. 13,231, 66 FR 53,063 (October 18, 2001), 3 C.F.R. (2001 comp.)

Executive Order No. 13,470, 73 FR 45,325 (August 4, 2008), 3 C.F.R. (2008 comp.)

Executive Order No. 13,636, 78 FR 11,739 (February 19, 2013), 3 C.F.R. (2013 comp.)

Facilitating cyber threat information sharing and partnering with the private sector to protect critical infrastructure: An assessment of DHS capabilities: Hearing before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies (H.R. hrg. 113-311), *U.S. House of Representatives*, 113th Cong. (2013). Retrieved July 17, 2013 from House of Representatives database: http://homeland.house.gov/hearing/subcommittee-hearing-facilitating-cyber-threat-information-sharing-and-partnering-private

Feickert, A. (2013, January 3). *The unified command plan and combatant commands: Background and issues for Congress* (Report No. R42077). Congressional Research Service; Washington D.C. Retrieved on June 24, 2013 from Homeland Security Digital Library: https://www.hsdl.org/?view&did=728232

Foreign Intelligence Surveillance Act of 1978. Pub. L. No. 95–511, 92 Stat. 1783, 50 U.S.C. § 1801 et seq. (2012).

Glossary of key information security terms. (2013, May 31). National Institue of Standards and Technology Interagency Report (IR) 7298: Revision 2. Retrieved August 26, 2013 from NIST: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Greenert, J. (2011, December). Navy 2025: Forward warfighters. *Proceedings, Vol. 137* (12) 1,306. Retrieved December 12, 2011, from web: http://www.usni.org/magazines/proceedings/2011–12

Greenwald, E. A. (2010, 31 August). History repeats itself: The 60-day cyberspace policy review in context. *Journal of National Security Law and Policy, 4* (1), 41–60. Retrieved February 21, 2013 from JNSLP Main Page via web: http://jnslp.com/wp-content/uploads/2010/08/05_Greenwald.pdf

Hayden, M. V. (2000). MEMORANDUM. National Security Service/Central Security Service. (October 2000). Retrieved January 23, 2013, from web: http://cryptome.org/nsa-reorg-et.htm

Hollis, D. (2011). Cyberwar case study: Georgia 2008. *Small Wars Journal*. Retrieved on June 04, 2013 from: http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Homeland Security Act (2002). Pub. L. No. 107–296, 116 Stat. 2135, 6 U.S.C. § 2147 et seq. *U.S. House of Representatives*, 107th Cong. (2002). Washington, DC: Government Printing Office, DOI: 25 November 2002. Retrieved December 04, 2011, from DHS database: http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

Homeland Security Presidential Directive 5 (HSPD-5). (2003). Department of Homeland Security. Washington, DC: Government Printing Office, DOI: 28 February 2003. Retrieved April 19, 2013, from the Homeland Security Digital Library: https://www.hsdl.org/?view&did=439105

Homeland Security Presidential Directive 7 (HSPD-7). (2003). Department of Homeland Security. Washington, DC: Government Printing Office, DOI: 17 December 2003. Retrieved December 01, 2011, from DHS database: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1

Homeland Security Presidential Directive 8 (HSPD-8). (2003). Department of Homeland Security. Washington, DC: Government Printing Office, DOI: 17 December 2003. Retrieved April 04, 2013, from Homeland Security Digital Library: https://www.hsdl.org/?view&did=441951

Jensen, E. (2010). Cyber warfare and precautions against the effects of attacks. *Texas Law Review, 88*(7), 1533–1569. Retrieved December 03, 2011, from ProQuest database: http://search.proquest.com/docview/722437496?accountid=12702

Joint Chiefs of Staff (JCS). (2012). Cyber incident handling program. *Chairman of the Joint Chiefs of Staff Manual 6510.01B,* (10 July 2012). Washington, DC: Government Printing Office. Retrieved July 19, 2013, from DTIC database: http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf

Joint Chiefs of Staff (JCS). (2010). Department of defense dictionary of military and associated terms. *Joint Publication 1–02,* (08 November 2010, amended 15 May 2011). Washington, DC: Government Printing Office. Retrieved Jan 17, 2013, from DTIC database: www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Joint Chiefs of Staff (JCS). (2009). J7 Joint Education and Doctrine Division (2009). *Joint doctrine update.* Washington, DC: Government Printing Office.

Joint Chiefs of Staff (JCS). (2008). Joint Operations (Change 1). *Joint Publication 3–0* (2008), Chapter III; Para 5(d). Washington, DC: Government Printing Office. Retrieved Jan 17, 2013, from DTIC database: www.dtic.mil/doctrine/new_pubs/jp3_0.pdf

Joint Chiefs of Staff (JCS). (2006). *National military strategy for cyberspace operations (2006)*; (Redacted Strategic Doctrine). Washington, DC: Government Printing Office, DOI: 11DEC2006. Retrieved December 12, 2011, from web: http://www.carlisle.army.mil/DIME/documents/National%20Military%20Strategy%20for%20Cyberspace%20Operations.pdf

Joint doctrine update: Joint chiefs of staff J7 joint education and doctrine division. (2009). *Joint Forces Quarterly, 55* (4), 176. Retrieved September 04, 2013, from DTIC database: http://www.dtic.mil/dtic/tr/fulltext/u2/a515171.pdf

Landau, S. (2013). Making sense from Snowden: What's significant in the NSA surveillance revelations. IEEE; *Security & Privacy: Safety-Critical Systems. Vol. 11*(4). (July/August 2013).

Lindsay, B. R. (2012). *Federal emergency management: A brief introduction.* Congressional Research Service Report for Congress; CRS No. R42845. (30 November 2012). Washington, DC: Government Printing Office. Retrieved May 28, 2013, from Homeland Security Digital Library: https://www.hsdl.org/?view&did=726902

Lynn, W. J. (III) (2010). Defending a new domain: The pentagon's cyberstrategy. *Foreign Affairs, 89*(5), 97–108. (September/October 2010). Retrieved May 16, 2013, from DTIC database: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA527707

Mandiant. (2013, February 19). *APT1: Exposing one of China's cyber espionage units*. Mandiant. (Online). Retrieved from Mandiant report database: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Mulligan, D., & Schneider, F. (2011). Doctrine for cybersecurity. Daedalus, 140(4), 70–92. Retrieved December 03, 2011, from ProQuest database: http://search.proquest.com/docview/903303254?accountid=12702

McAfee. (2013, July). *Economic impact of cybercrime and cyber espionage*. Center for Strategic and International Studies. Washington D.C.: McAfee, Inc. (2013). Retrieved July 29, 2013 from CSIS database: http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

National Commission on Terrorist Attacks. (2004). *The 9/11 commission report: Final report of the National Commission on Terrorist Attacks upon the United States*. New York: W.W. Norton. (2004). Retrieved January 28, 2013, from Government Publication Office database: http://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf

National cybersecurity workforce framework. (2013, March).National Institute of Standards and Technology. Retreived August 26, 2013 from NIST Library: http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_interactive.pdf

National disaster recovery framework. (2011). Department of Homeland Security. Washington, DC: Government Printing Office. (September 2011). Retrieved May 28, 2013 from Homeland Security Digital Library: https://www.hsdl.org/?view&did= 687785

National information assurance (IA) glossary. (2012, April 26). Committee on National Security Systems (CNSS) Instruction No. 4009. Retrieved August 26, 2013 via: http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

National infrastructure protection plan (NIPP). (2009). *Defense industrial base sector-specific plan (Annex).* Department of Defense (2010). Washington, DC: Government Printing Office. (2012). Retrieved December 04, 2011, from DHS database: http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf

National mitigation framework. (2013). Department of Homeland Security. Washington, DC: Government Printing Office. (May 2013). Retrieved May 15, 2013 from Homeland Security Digital Library: https://www.hsdl.org/?view&did=736015

National preparedness system. (2011). Department of Homeland Security (2011). Washington, DC: Government Printing Office. (November 2011). Retrieved May 09, 2013, from FEMA database: http://www.fema.gov/library/file;jsessionid=2A6F38469C17DA7CFFAC8B628819B048.WorkerPublic2?type=publishedFile&file=national_preparedness_system_final.pdf&fileid=b1608f80–16c5–11e2–956e-001cc456982e

National prevention framework. (2013). Department of Homeland Security. Washington, DC: Government Printing Office. (May 2013). Retrieved May 15, 2013 from Homeland Security Digital Library: https://www.hsdl.org/?view&did=736093

National response framework. (2008). Department of Homeland Security. Washington, DC: Government Printing Office. (January 2008). Retrieved May 15, 2013 via FEMA Home page: www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

National response framework (2nd Ed.). (2013). Department of Homeland Security. Washington, DC: Government Printing Office. (May 2013). Retrieved May 15, 2013 from Homeland Security Digital Library: https://www.hsdl.org/?view&did=735934

National Security Act of 1947. 61 Stat. 495 (July 26, 1947), 50 U.S.C. §401 et seq..

National Security Directive 1 (NSD-1). (1989, January 31). *Organization of the national security council system.* Office of the President of the Unitied States. Washington, DC: Government Printing Office, Declassified: 10 May 1995. Retrieved November 17, 2012 from the Federation of American Scientists homepage via: http://www.fas.org/irp/offdocs/nsd/nsd1.pdf

National Security Directive 10 (NSD-10). (1989, May 7). *Creation of New Policy Coordinating Committees*. Office of the President of the Unitied States. Washington, DC: Government Printing Office, Declassified: 18 October 1995. Retrieved January 17, 2013 from the Federation of American Scientists homepage via: http://www.fas.org/irp/offdocs/nsd/nsd10.pdf

National Security Directive 42 (NSD-42). (1990, July 5). *National policy for the security of national security telecommunications and information systems*. Office of the President of the Unitied States. Washington, DC: Government Printing Office, Declassified: 22 November 1996. Retrieved July 29, 2013 from the Federation of American Scientists homepage via: http://www.fas.org/irp/offdocs/nsd/nsd42.pdf

National strategy to secure cyberspace. (2003, February). President's Critical Infrastructure Protection Board. Washington, DC: Government Printing Office. Retrieved May 28, 2013 via Department of Defense database: http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberspace_strategy%5B1%5D.pdf

Navy Warfare Publication 3–32; Maritime Operations at the Operational Level of War (2008). Chapter 5 et seq.

Obama, B., (2009, May 29). Remarks by the President on securing our nation's cyber infrastructure. White House: Office of the Press Secretary – Televised Public Statement. Retrieved May 05, 2013 from Whitehouse Main Page: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

Office of Management and Budget (2012). *Budget of the United States government. Fiscal Year 2013: Analytical Perspectives*, February 2012, Appendix – Homeland Security Mission Funding by Agency and Budget Account. Washington, DC: Government Printing Office. (2012). Retrieved January 24, 2013, from Whitehouse Main Page via web: http://www.whitehouse.gov/sites/default/files/omb/budget/fy2013/assets/homeland_supp.pdf

Paine, T. (1776). *Common sense*. Philadelphia: printed. Sold by W. and T. Bradford [1776]. Retrieved February 26, 2013 from web: http://www.ushistory.org/paine/commonsense

Painter, W. J. (2013, February 27). *Issues in homeland security policy for the 113th congress* (Report No. R42985). Congressional Research Service; Washington D.C. Retrieved on July 30, 2013 from Homeland Security Digital Library: https://www.hsdl.org/?view&did=732600

Perlroth, N., & Sanger, D.E. (2013, March 28). Cyberattacks seem meant to destroy, not just disrupt. *The New York Times*. New York. Retrieved June 18, 2013 from NYT Main Page: http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html?pagewanted=all&_r=0

Posse Comitatus Act of 1878. 20 Stat. 152 (June 18, 1878). 18 U.S.C. §1385.

Post-Katrina Act of 2006. Pub. L. No. 109–295. 120 Stat. 1424–1433. 6 U.S.C. §741-764.

Presidential Decision Directive 39 (Declassified). (1995). Office of the President of the United States. Washington, DC: Government Printing Office, DOI: 21 June 1995. Retrieved May 13, 2013 from web: http://www.fas.org/irp/offdocs/pdd/pdd-39.pdf

Presidential Policy Directive 8. (2011). Office of the President of the United States. Washington, DC: Government Printing Office, DOI: 30 March 2011. Retrieved February 05, 2013 from web: http://www.fas.org/irp/offdocs/ppd/ppd-8.pdf

Presidential Policy Directive 20. (2012). Office of the President of the United States. Washington, DC: JWICS, DOI: 24 November 2012.

Reese, S. (2013, January 8). *Defining homeland security: Analysis and congressional considerations* (Report No. R42462). Congressional Research Service; Washington D.C. Retrieved January 24, 2013 from Homeland Security Digital Library: https://www.hsdl.org/?view&did=728387

Reorganization Plan No. 3 of 1978, 43 FR 41,943, 3 C.F.R. (1978 comp.), p. 329

Rogers M. (2013, February 14). Statement to the U.S. House, Permanent Select Committee on Intelligence, Open Hearing: Cyber Threats and Ongoing Efforts to Protect the Nation, Hearing. Retrieved June 11, 2013, from http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/RogersOpening02142013.pdf

Rutkowski, A. (2010). Lessons from the first great cyberwar era. *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 12*(1), 5–9. Retrieved December 08, 2011, from ProQuest database: http://search.proquest.com.libproxy.nps.edu/docview/275005515/fulltextPDF/1338461D512746AB486/1?accountid=12702

Securing cyberspace for the 44th presidency. (2008, December). Commission on Cybersecurity for the 44th Presidency; Center for Strategic and International Studies; Washington D.C. Retrieved April 24, 2013 from CSIS Digital Library: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Security in cyberspace: Hearing before the U.S. senate permanent subcommittee on investigations. 104th Cong. (5 June 1996). Retrieved May 13, 2013 via web: http://www.fas.org/irp/congress/1996_hr/s9606051.htm

Sharp, W. G. (Sr.) (2012, 16 February). *Information and cyberspace operations.* Pentagon Professional Development Breifing Prepared for the Office of the Deputy Assistant Secretary of Defense for Cyber Policy, Slide 12.

Sharp, W. G. (Sr.) (2010, 31 August). The past, present, and future of cybersecurity. *Journal of National Security Law and Policy 4*(1), 13–26. Retrieved February 20, 2013 from JNSLP Main Page via web: http://jnslp.com/2010/08/13/the-past-present-and-future-of-cybersecurity

Stafford Act of 1988. 102 Stat. 4689. 1 U.S.C. §103(a) et seq. (1988). Robert T. Stafford disaster relief and emergency assistance act (Stafford Act) of 1988. DOI: 23 November 1988. U.S. Congress (1988); Pub. L. No. 93–288 as amended by Pub. L. No. 100–707. Retrieved May 03, 2013, from Homeland Security Digital Library: https://www.hsdl.org/?view&did=480391

Strategic National Risk Assessment. (2011, December). *The strategic national risk assessment in support of PPD 8: A comprehensive risk-based approach toward a secure and resilient nation.* Department of Homeland Security (2011). Washington, DC: Government Printing Office. Retrieved May 09, 2013 from DHS database: http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf

Talbott, S. (1991, August 5). Mikhail Gorbachev and George Bush: The summit goodfellas. *Time Magazine*. New York, NY: Time Inc. Retrieved April 30, 2013 from Time Magazine Main Page via web: http://www.time.com/time/magazine/article/0,9171,973554–5,00.html

Tikk, E. (2010). Global cybersecurity-thinking about the niche for NATO. *SAIS Review, 30*(2), 105–119. Retrieved December 08, 2011, from ProQuest database: http://search.proquest.com/docview/859361196?accountid=12702

U.S. Constitution (1787). Washington, DC: Government Printing Office, (Document No. 110–50). (Reproduced: July 25, 2011). Retrieved July, 20, 2013 from the Government Printing Office web page via: http://www.gpo.gov/fdsys/pkg/CDOC-110hdoc50/pdf/CDOC-110hdoc50.pdf

U.S. Department of Homeland Security (2010, February 19). *Computer network security & privacy protection.* Retrieved July 19, 2013 from DHS database: http://www.dhs.gov/xlibrary/assets/privacy/privacy_cybersecurity_white_paper.pdf

U.S. Department of Homeland Security (2011). *Implementing 9/11 commission report recommendations: Progress report 2011.* Retrieved February 07, 2013 from DHS database: http://www.dhs.gov/xlibrary/assets/implementing-9–11-commission-report-progress-2011.pdf

U.S. Department of Homeland Security (2004). *National response plan* (December 2004). Retrieved December 01, 2011 from DHS database: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

U.S. Department of Homeland Security (2012, July 11). *National security deployment.* National Cybersecurity Protection System briefing to DHS Data Privacy and Integrity Advisory Committee (PPT; Oct 31, 2012). Retrieved July 19, 2013 from DHS database: http://www.dhs.gov/sites/default/files/publications/privacy/DPIAC/NCPS%20Overview_DPIAC_31OCT2012.pdf

U.S. Department of Homeland Security (2012, August). *Office of infrastructure protection strategic plan: 2012-2016.* Retrieved July 19, 2013 from DHS database: https://www.dhs.gov/sites/default/files/publications/IP%20Strategic%20Plan%20FINAL.pdf

U.S. Department of Homeland Security (2009). Partnering to enhance protection and resiliency. *National Infrastructure Protection Plan* (2009). Retrieved December 01, 2011 from DHS database: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

U.S. Department of Homeland Security (2013, April 19). *Privacy impact assessment for EINSTEIN 3–Accelerated (E3A).* National Protection and Programs Directorate; Office of Cybersecurity & Communications; Network Security Deployment Branch. Retrieved July 29, 2013 from DHS database: http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf

U.S. Department of Justice (2012, November 14). Blog: New network takes aim at cyber threats to national security. Department of Justice, Online. Retrieved July 26, 2013 from DOJ homepage: http://blogs.justice.gov/main/archives/2558

U.S. Department of Justice (2012, February 9). *Department of justice: Strategic plan for fiscal years 2012-2016.* Retrieved July 26, 2013 from DOJ homepage: http://www.justice.gov/jmd/strategic2012-2016/DOJ-Strategic-Plan-2-9-12.pdf

U.S. Government Accountability Office (1993, July). *Disaster management, improving the nation's response to catastrophic disasters,* Report to Congressional Requesters. (Publication No. GAO/RCED-93–186), 1. Retrieved April 19, 2013 from GAO Reports Main Page via GPO Access database: http://archive.gao.gov/t2pbat5/149631.pdf

U.S. Government Accountability Office (2011, July). *Defense department cyber efforts: DOD faces challenges in its cyber activities.* Report to Congressional Requesters (Publication No. GAO-11–75), *U.S. House of Representatives,* 111th Cong. (2011). Retrieved December 02, 2011 from GAO Reports homepage via GPO Access database: http://www.gao.gov/products/GAO-11–75

U.S. Government Accountability Office (2011, 26 July). *Cybersecurity: Continued attention needed to protect our nation's critical infrastructure*. Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce (Publication No. GAO-11–865T), *U.S. House of Representatives*, 111th Cong. 1 (2011). Retrieved December 02, 2011 from GAO Reports Main Page via GPO Access database: http://www.gao.gov/products/GAO-11–865T

U.S. Government Accountability Office (2011, 29 July). *Defense department cyber efforts: definitions, focal point, and methodology needed for DOD to develop full-spectrum cyberspace budget estimates.* Briefing for the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services (Publication No. GAO-11–695R), *U.S. House of Representatives*, 111th Cong. 1 (2011). Retrieved December 02, 2011 from GAO Reports Main Page via GPO Access database: http://www.gao.gov/products/GAO-11–695R

U.S. Government Accountability Office (2012). *DOD Needs to address gaps in homeland defense and civil support guidance.* Report to Senate Committee on Homeland Security and Government Affairs (Publication No. GAO-13–128), *U.S. Senate*, 112th Cong. (2012). Retrieved December 02, 2011 from GAO Reports Main Page via GPO Access database: http://www.gao.gov/products/GAO-13–128

U.S. Government Accountability Office (2013). *Cybersecurity: National strategy, roles, and responsibilities need to be better defined and more effectively implemented.* Report to Senate Committee on Homeland Security and Government Affairs (Publication No. GAO-13–187), *U.S. Senate*, 112th Cong. (2013). Retrieved February 26, 2013 from GAO Reports Main Page via GPO Access database: http://www.gao.gov/products/GAO-13–187

USA Patriot Act of 2001, 18 U.S.C. § 272 et seq. (2001). Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism act (USA Patriot Act) of 2001. DOI: 26 October 2001. U.S. Congress (2001); Pub. L. No. 107–56. Retrieved December 02, 2011 from Homeland Security Digital Library: https://www.hsdl.org/?view&did=537

von Clausewitz, C. (1989). On War (1st Edition); ed., trans. Michael Howard and Peter Paret, Princeton, NJ: Princeton University Press, 593.

Wall, A. E. (2011). Demystifying the title 10-title 50 debate: Distinguishing military operations, intelligence activities & covert action. *Harvard National Security Journal, 3*, 84-141. Retrieved July 30, 2013 via: http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Wall1.pdf

War Powers Resolution (1973). Pub. L. No. 93-148, 87 Stat. 555 (1973), 50 U.S.C. §1541–1548.

Warner, M. (2007). Wanted: A definition of “intelligence”: Understanding our craft, *Studies in Intelligence, 46*(3), 1. Retrieved April 20, 2013 from CIA Main Page: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html#fn7

White House (2009, 09 February). President Obama directs the national security and homeland security advisors to conduct immediate cyber security review. White House: Office of the Press Secretary–Public Statement. (2009). Retrieved February 20, 2013 from Whitehouse Main Page: http://www.whitehouse.gov/the_press_office/advisorstoconductimmediatecybersecurityreview

Whittaker, A., Brown, S., Smith, F., & McKune, E. (2011, 15 August). *The national security policy process: The national security council and interagency system*. Retrieved July 20, 2013 from National Defense University main page via web: http://www.ndu.edu/es/outreach/publications/nspp/docs/icaf-nsc-policy-process-report-08–2011.pdf

Yoo, J. C. (2001, September 25). *Memorandum opinion for the deputy counsel to the president*. Retrieved July 20, 2013 from U.S. Department of Justice main page: http://www.justice.gov/olc/warpowers925.htm#N_11_

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California